ANNUAL REPORT TO THE CONGRESS ON THE INFORMATION SHARING ENVIRONMENT

Prepared by the
Program Manager, Information Sharing Environment

Report Documentation Page

Form Approved
OMB No. 0704-0188

1. REPORT DATE	2. REPORT TYPE	3. DATES COVERED
JUN 2008		**00-00-2008 to 00-00-2008**

4. TITLE AND SUBTITLE	5a. CONTRACT NUMBER
Annual Report to the Congress on the Information Sharing Environment	5b. GRANT NUMBER
	5c. PROGRAM ELEMENT NUMBER
6. AUTHOR(S)	5d. PROJECT NUMBER
	5e. TASK NUMBER
	5f. WORK UNIT NUMBER
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) **Office of the Director of National Intelligence ,Program Manager,Information Sharing Environment,Washington,DC**	8. PERFORMING ORGANIZATION REPORT NUMBER
9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)	10. SPONSOR/MONITOR'S ACRONYM(S)
	11. SPONSOR/MONITOR'S REPORT NUMBER(S)

12. DISTRIBUTION/AVAILABILITY STATEMENT
Approved for public release; distribution unlimited

13. SUPPLEMENTARY NOTES

14. ABSTRACT

15. SUBJECT TERMS

16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT	18. NUMBER OF PAGES	19a. NAME OF RESPONSIBLE PERSON
a. REPORT	b. ABSTRACT	c. THIS PAGE			
unclassified	**unclassified**	**unclassified**	**Same as Report (SAR)**	**74**	

ANNUAL REPORT TO THE CONGRESS ON THE INFORMATION SHARING ENVIRONMENT

Prepared by the
Program Manager, Information Sharing Environment

June 30, 2008

TABLE OF CONTENTS

LIST OF FIGURES

LIST OF TABLES

Foreword

Message From the Program Manager, Information Sharing Environment

On behalf of the President and the Director of National Intelligence, I am pleased to present this second *Annual Report to the Congress on the Information Sharing Environment (ISE)*. We believe it demonstrates a solid record of accomplishment by the Office of the Program Manager, the many agencies represented on the Information Sharing Council, and our partners in State, local, and tribal (SLT) governments. In the past year we have made significant progress in a number of important areas of information sharing. Issuance of a new framework for marking and handling Controlled Unclassified Information, establishment of the Interagency Threat Assessment and Coordination Group at the National Counterterrorism Center, completion of a functional standard for terrorism-related suspicious activity reporting, and publication of the first version of an enterprise architecture framework for the ISE are only a few of the important achievements.

Notwithstanding these achievements, there is still much more to be done. In particular, Information Sharing Council (ISC) member agencies must work to fully implement the ISE; assure full participation by our SLT partners; and help secure and make safe our communities and nation by effectively sharing information. So, in addition to describing 2007-08 accomplishments, the Report outlines the status, outcomes and activities that are needed to continue to improve information sharing.

Thomas E. McNamara
Program Manager, Information Sharing Environment

Executive Summary

This second *Annual Report to the Congress on the Information Sharing Environment (ISE)* is submitted in accordance with requirements in Section 1016(h) of *the Intelligence Reform and Terrorism Prevention Act of 2004*, as amended (IRTPA).[1] This Report describes the state of the ISE, highlights areas where there has been measurable progress in improving information sharing, and demonstrates the value of the ISE to the Nation's broader counterterrorism (CT) mission. In particular, the President's October 2007 *National Strategy for Information Sharing* (NSIS) reinforced the importance of information sharing as a national priority. The NSIS integrates all prior terrorism-related information sharing policies, directives, plans, and recommendations and provides a national framework against which to implement the ISE.

The enactment of IRTPA in December 2004 signaled the start of a major effort to ensure that barriers to information sharing were removed and that best practices were employed across Federal agencies. While the complexity of the information-sharing challenge should not be underestimated, significant progress has been made. This Report addresses progress in information sharing to date while revealing how the paradigm of information sharing – and the ISE in particular – has broadly permeated our institutions of government.

ISE accomplishments are significant when viewed according to the original mandate, set forth in the President's December 16, 2005 *Memorandum to the Heads of Executive Departments and Agencies on the Guidelines and Requirements in Support of the Information Sharing Environment,* which set forth the Presidential Information Sharing Guidelines. These guidelines are implemented by leveraging ongoing information sharing efforts and supported by promoting a culture of information sharing.

Implementation of Presidential Information Sharing Guidelines

As of this Report, recommendations for the five Presidential guidelines are complete and approved by the President for implementation, and actual implementation is well underway across all five areas. The following is a summary of that status; additional details are provided in the body of this Report.

[1] *Intelligence Reform and Terrorism Prevention Act of 2004* (IRTPA), as amended, P.L. 108-458 (December 17, 2004) §1016(b)(1)(A). The scope of the ISE was originally limited to "terrorism information" as defined in Section 1016. In August 2007, The *Implementing Recommendations of the 9/11 Commission Act of 2007* (P.L. 110-53), included amendments to Section 1016 that expanded the scope of the ISE to explicitly include homeland security and weapons of mass destruction information and identified additional ISE attributes. It also endorsed and formalized many of the recommendations developed in response to the Presidential information sharing guidelines, such as the creation of the Interagency Threat Assessment and Coordination Group, and the development of a national network of State and major urban area fusion centers.

1. *Defining Common Standards for How Information is Acquired, Accessed, Shared, and Used within the ISE*. In October 2007, the Office of the Program Manager for the Information Sharing Environment (PM-ISE) and the interagency Information Sharing Council (ISC) formally established the Common Terrorism Information Sharing Standards (CTISS) Program. The first common ISE standard (the *ISE Suspicious Activity Reporting (SAR) Functional Standard*) was issued in January 2008 and others are under development. In direct response to IRTPA direction, the PM-ISE released the *ISE Enterprise Architecture Framework* (ISE EAF) last fall. The ISE EAF provides a common architectural structure for agencies to use as they implement these information sharing standards.

2. *Developing a Common Framework for the Sharing of Information Between and Among Executive Agencies and State, Local, and Tribal (SLT) Governments, Law Enforcement Agencies, and the Private Sector*. Established at the National Counterterrorism Center (NCTC), an Interagency Threat Assessment and Coordination Group (ITACG) facilitates the production of "federally coordinated" terrorism-related information products intended for dissemination to SLT officials and private sector partners. Considerable progress has also been achieved at developing a national network of state and major urban area fusion centers.

3. *Standardizing Procedures for Sensitive But Unclassified (SBU) Information*. Developed by an interagency Coordinating Committee and implemented through the President's May 9, 2008 *Memorandum for the Heads of Executive Departments and Agencies on the Designation and Sharing of Controlled Unclassified Information (CUI),* a common framework will streamline the designation, marking, safeguarding, and dissemination of CUI within the ISE.[2]

4. *Facilitating Information Sharing Between Executive Agencies and Foreign Partners*. In March 2008, the PM-ISE and ISC established an interagency committee to guide implementation of these recommendations. The committee provides tools and other mechanisms to assist Federal agencies in developing and managing foreign sharing agreements.

5. *Protecting the Information Privacy Rights and Other Legal Right of Americans*. ISE Privacy Guidelines and implementing procedures have been issued, and an ISE Privacy Guidelines Committee (PGC) established, to assist agencies in implementation. Released by the PM-ISE in the fall of 2006, the promulgated guidelines maintain and build upon existing privacy protections while continuing

[2] *Memorandum for the Heads of Executive Departments and Agencies: Designation and Sharing of Controlled Unclassified Information (CUI),* White House (May 9, 2008). Available online at: http://www.whitehouse.gov/news/releases/2008/05/20080509-6.html.

to enhance the sharing of terrorism-related information between agencies at all levels of government.[3]

Leveraging Ongoing Information Sharing Efforts

The PM-ISE, in consultation with the ISC, has identified and leveraged ongoing information sharing efforts to align with the Presidential Guidelines and extended these efforts to cover all ISC participant agencies. The PM-ISE has also worked with agencies to build their capacity for information sharing by having agencies take greater ownership of these efforts, and ultimately, of targeted outcomes and out-year performance goals. The PM-ISE has leveraged, enhanced, and extended various existing initiatives, to include:

- Information sharing frameworks and data standards, including the National Information Exchange Model (NIEM) standards and Department of Defense (DoD)-Director of National Intelligence (DNI) Universal Core (UCORE) data standards, as part of the CTISS Program, to facilitate information exchanges (i.e. ISE SAR information) between different domains or communities of interest;
- The Federal Bureau of Investigation (FBI)-sponsored Joint Terrorism Task Forces (JTTFs), combining Federal-State-Local units dedicated to combating terrorism in specific geographical areas;
- State and major urban area fusion centers, many of which are collocated with JTTFs and some of which have Department of Homeland Security (DHS) representation as well; and
- The ISE Governance Structure (described in the ISE Implementation Plan) that provides a framework for coordinating interagency actions and leveraging existing or planned agency initiatives; and
- Federal, SLT, and private sector governance structures such as the Federal Chief Information Officers Council, the Global Justice Information Sharing Initiative (Global), and the National Infrastructure Protection Plan sector partnership model, as mechanisms to provide subject matter expertise and contribute to the development of ISE capabilities.

Sound ISE investment oversight and planning are important parts of managing the ISE and leveraging ongoing information sharing efforts. Coordinated, cross-ISE investment planning provides insight into ISC members' programs and budgets and will help ensure that ISC member agencies include ISE initiatives in their out-year planning and investment efforts. As detailed in Section 7, a standard *ISE Planning Cycle* coordinates the ISE's strategic direction, resource planning, and program oversight. It leverages existing Office of Management and Budget (OMB) processes and procedures to include

[3] *ISE Privacy Guidelines,* the Office of the Program Manager for the Information Sharing Environment (December 4, 2006). Available online at: http://www.ise.gov/docs/privacy/PrivacyGuidelines20061204.pdf.

the steps involved in planning, programming, budgeting, and executing the resources necessary to institutionalize the ISE. Annual ISE investment reviews focus on identifying information sharing costs from larger mission operations costs to ensure that existing resource allocations are properly leveraged as part of the investment planning process.

Promoting a Culture of Information Sharing

Organizational cultures across the ISE vary widely, and information sharing is not viewed across the board as a required behavior. To promote a shared awareness of the ISE and encourage such behavior, the PM-ISE will issue an "ISE 101" training module this summer. The course is intended to give a common understanding of the ISE to all employees who support the CT mission. This training, coupled with continued efforts to include information sharing as a formal evaluation factor in personnel performance reports and agency incentive programs, is designed to help move the traditional "need to know" culture to one based on a "responsibility to provide."[4]

Way Ahead

In addition to chronicling the progress made since September 11th in improving information sharing, the NSIS outlines the steps necessary to ensure that agencies continue to embrace the practice of freely sharing terrorism-related information. In the next year, key milestones include delivery of:

- Functional and technical standards, including a focus on fully-implementing a national standardized process for ISE SAR;
- Technical assistance, training, and policy that furthers the establishment and operational effectiveness of a national integrated network of fusion centers;
- A process that fully aligns ISE budget, planning, and performance activities to OMB and agencies' management and budget processes;
- An implementation plan for the new CUI framework; and
- The continued protection of the privacy and other legal rights of all Americans through further implementation of the ISE Privacy Guidelines.

[4] *United States Intelligence Community Information Sharing Strategy,* the Office of the Director of National Intelligence (February 2008), p. 2.

1 Introduction

1.1 Purpose and Scope

This second *Annual Report to the Congress on the Information Sharing Environment (ISE)* is submitted in accordance with requirements in Section 1016(h) of the *Intelligence Reform and Terrorism Prevention Act of 2004, as amended* (IRTPA).[5] This Report describes the state of the ISE, highlights areas where there has been measurable progress in improving information sharing, and demonstrates the value of the ISE to the Nation's broader counterterrorism (CT) mission. In particular, the President's October 2007 *National Strategy for Information Sharing* (NSIS) reinforced the importance of information sharing as a national priority. The NSIS integrates all prior terrorism-related information sharing policies, directives, plans, and recommendations and provides a national framework against which to implement the ISE.

This Report responds directly to the IRTPA requirement for "a progress report on the extent to which the ISE has been implemented." It reflects the collective accomplishments and challenges of an information sharing partnership of Federal and non-Federal stakeholders vested in the improvement of terrorism-related information sharing. It also highlights individual agency initiatives that stand out as best practices in information sharing and help form the fabric of the ISE.

1.2 Overview of the ISE

1.2.1 Background

Section 1016 of IRTPA defines the ISE as "an approach that facilitates the sharing of terrorism and homeland security information" which "may include any methods determined necessary and appropriate for carrying out this section."[6] The ISE Implementation Plan (IP) sets forth a vision of the environment as "a trusted partnership between all levels of government in the United States, the private sector, and our foreign partners, to detect, prevent, disrupt, preempt, and mitigate the effects of

[5] IRTPA, as amended, op. cit., §1016(b)(1)(A). The scope of the ISE was originally limited to "terrorism information" as defined in Section 1016. In August 2007, The *Implementing Recommendations of the 9/11 Commission Act of 2007* (P.L. 110-53), included amendments to Section 1016 that expanded the scope of the ISE to explicitly include homeland security and weapons of mass destruction information and identified additional ISE attributes. It also endorsed and formalized many of the recommendations developed in response to the Presidential information sharing guidelines, such as the creation of the Interagency Threat Assessment and Coordination Group, and the development of a national network of State and major urban area fusion centers.

[6] Ibid. §1016(a)(2).In the balance of this report, terrorism and homeland security information will be referred to as "terrorism-related information."

terrorism against the territory, people, and interests of the United States of America by the effective and efficient sharing of terrorism information."[7]

These broad descriptions convey the essential point that establishing the ISE is not about building a dedicated information system to support the national CT mission. Rather, it largely entails building on capabilities already in place by adjusting and integrating existing policies, business processes, architectures, standards, and systems to enable the improved sharing of information among all ISE participants. The authors of IRTPA carefully avoided calling the ISE a "system," "information sharing network," or "program," choosing instead the term "environment" to describe the set of conditions that must coalesce through the application of those interrelated policies, business processes, and standards to use existing systems.[8]

1.2.2 The ISE: A Partnership of Five Communities

The ISE IP describes the five primary communities that constitute the ISE: Intelligence, Foreign Affairs, Homeland Security, Law Enforcement, and Defense. To illustrate further, Figure 1-1 depicts these five communities as multi-story buildings within a common neighborhood which contain repositories of terrorism-related information and are connected by walkways and skyways.[9] Each building (representing a single community) also has several distinct but connected floors corresponding to the stakeholders who contribute to that community's counterterrorism efforts—Federal and State, local, and tribal (SLT) governments, private sector entities, and foreign partners. The figure illustrates that stakeholder relationships will vary from one community to another. The Homeland Security community, for example, has a stronger association with SLT and private sector stakeholders than does the Foreign Affairs community which, in turn, must necessarily have much closer ties with foreign partners.

The inner courtyard of Figure 1-1 depicts the essential capabilities that help unify the five communities. Improved policies, business processes, architectures, standards, and systems combine to enable the walkways, skyways, elevators, and staircases of the ISE to provide trusted, efficient, and effective movement of information both inside the buildings and across the neighborhood.

---

7 *ISE Implementation Plan* (November 2006), p. 11.

8 The second Markle Foundation Task Force report, *Creating a Trusted Information Network for Homeland Security* (December 2002) did use the term "network." IRTPA, however, although influenced by the Markle report, eschewed this term in favor of "environment."

9 Both Intelligence Community members and other organizations (sometimes referred to as non-Title 50 agencies) will contribute to these repositories of terrorism-related information.

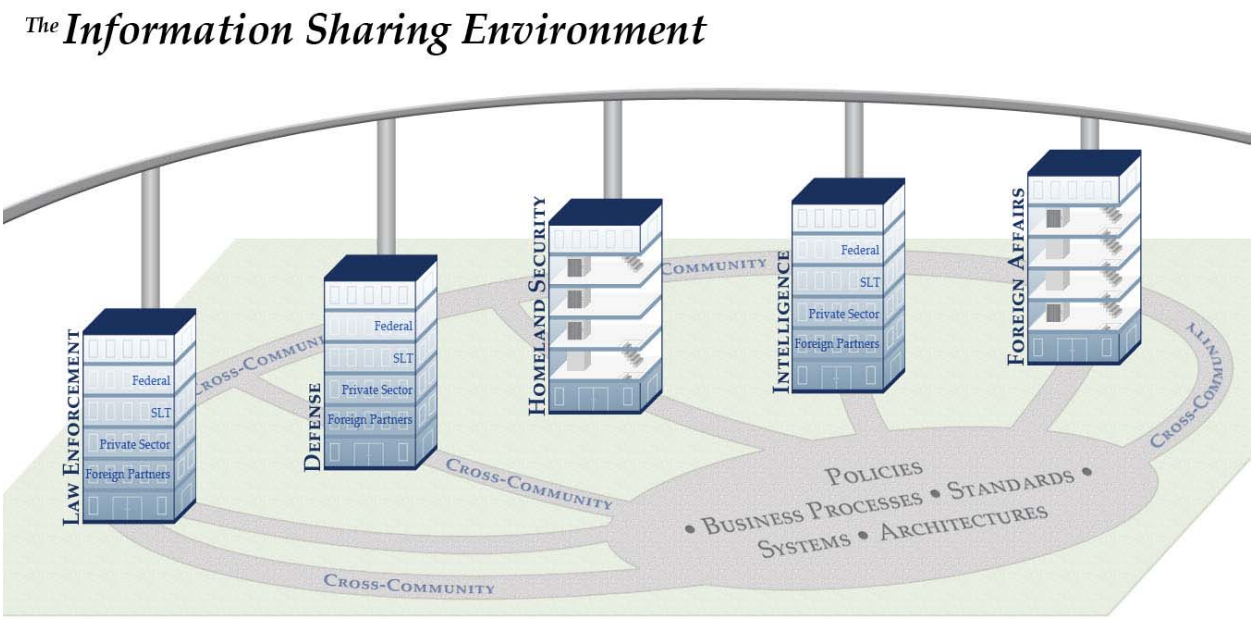


Figure 1-1. View of the ISE as a Partnership of Five Communities

The purpose of the ISE is to *rationalize, standardize, and harmonize* the policies, business processes, architectures, standards, and systems used to share information. Although the ISE strives for much uniformity as possible, actual implementation will vary from one building (community) to another (and even between floors in a building) depending on varied mission needs and immediate capabilities. State and local processes and policies, for example, will not be identical to those of the Federal Government. Nor will the needs of a small town be the same as those of a major urban area. Accordingly, rather than striving to develop identical implementations across the ISE, the intent is to achieve *mostly common* capabilities—based on a common architectural framework supplemented by mostly common laws, regulations, policies, business processes, architectures, standards, and systems—but tailored to ISE participant needs. These capabilities are developed in consultation with the Information Sharing Council (ISC), an interagency advisory body chaired by the Program Manager, Information Sharing Environment (PM-ISE) where participants from each of the five communities help manage and implement the ISE.

1.2.3 Achieving ISE Operational Capabilities

ISE progress is a function of identifying, prioritizing, and measuring continuous improvements to operational capabilities by modifying processes or creating new ones, issuing guidance and standards to ISE participants, providing demonstrable evidence of the effects of these changes through selected information sharing pilots and evaluation environments, and incorporating these improvements into established agency investment and resource management processes.

Achieving the desired outcome and managing the ISE's performance requires a common understanding regarding the problems to be solved, the essential capabilities that constitute the ISE, and the actions needed to ensure that these capabilities are developed and deployed in a manner "consistent with national security and with applicable legal standards relating to privacy and civil liberties."[10] The original blueprint upon which the work of the ISE is based is set forth in the President's December 16, 2005 *Memorandum to the Heads of Executive Departments and Agencies on the Guidelines and Requirements in Support of the Information Sharing Environment,* was further refined in the ISE IP, and fully synthesized in the NSIS. These Presidential guidelines describe ISE capabilities in terms of interrelated policies, business processes, architectures, standards, and systems that, taken together, constitute the sharing environment envisioned in IRTPA and the NSIS—the elements depicted in the courtyard of Figure 1-1.

1.3 The Reality of an Information Sharing Environment

The NSIS requires that the ISE support inclusion of locally generated information because such information is important to the development of statewide and national assessments of terrorist threats.[11] The intent is to make all available information on terrorist-related suspicious activity more widely available to ISE members while protecting information privacy and the legal rights of Americans.

Two important institutions that have spurred progress in enhanced Federal and SLT sharing are:

- The Federal Bureau of Investigation (FBI)-sponsored Joint Terrorism Task Forces (JTTFs), combining Federal-State-Local units dedicated to combating terrorism in specific geographical areas; and
- State and major urban area fusion centers, many of which are collocated with JTTFs, and some of which have Department of Homeland Security (DHS) representation as well.

JTTFs and fusion centers represent a change in culture and a willingness to share information across several levels of government. Both are partnerships that rely on new policies, business processes, architectures, standards, and systems that provide users the ability to access and search information in different databases. Both Federal and SLT law enforcement agencies recognized that they needed to begin to share more detailed information to be effective. This awareness has resulted in the mutual agreement by trusted partners to exchange actual operational data reports, case files, and similar information on both open and closed investigations.

[10] IRTPA, as amended, op cit., §1016(b)(1)(A).

[11] *National Strategy for Information Sharing* (October 2007), pp. A1-6 and A1-7.

This level of sharing required governance boards to develop inter-agency agreements, policies, business processes, and standards—which eventually led to the development of systems requirements. The organizations involved all supported solutions that used distributed sharing methods, allowing each organization to retain its own information and, at the same time, make it available for others to search and retrieve. A distributed approach allows organizations to add, update, or purge data based on all applicable laws and guidance. For example, a State may be able to broadly share information on terrorist-related suspicious activity, but may have to restrict access to certain fields to comply with State privacy laws. Since this information is usually maintained in different formats by each organization, the Law Enforcement Information Sharing Program (LEISP) Exchange Specification (LEXS)—a subset of the National Information Exchange Model (NIEM)— was developed to serve as an "interpreter" between different law enforcement systems, enabling participants on one system to obtain results from others in a familiar format.

At the Federal level, the FBI's Law Enforcement On-line (LEO) system has provided a protected means for sharing Sensitive But Unclassified (SBU) data with regional law enforcement (LE) agency partners through a project originally known as Regional Data Exchange (R-DEx) and subsequently adopted by the Department of Justice (DOJ) for all of its components and renamed OneDOJ. Using LEO, DOJ is integrating the OneDOJ regional partnerships with a new Law Enforcement National Data Exchange (N-DEx) program under the FBI Criminal Justice Information Services (CJIS) Division. In addition, DOJ supports six Regional Information Sharing System (RISS) Network centers that provide tailored support for specialized LE functions to meet regional needs.

The N-DEx development clearly illustrates the value of using common standards. Under N-DEx, exchange of information between law enforcement agencies and CJIS is accomplished by using NIEM standards. In fact, CJIS developed the Information Exchange Package Description (IEPD) before releasing the N-DEx Request for Procurement, allowing the standard to drive subsequent development and implementation activities. Although specific dollar savings are difficult to quantify, vendors are now packaging N-DEx-NIEM compliant applications into off-the-shelf solutions than can easily be adopted by additional jurisdictions, effectively amortizing development costs across a broader customer base.

The Naval Criminal Investigative Service (NCIS) also established the Law Enforcement Information Exchange (LInX) that offers local or regional data hosting capabilities for SLT law enforcement agencies to support their sharing efforts. In the past year, DHS's Immigration and Customs Enforcement (ICE) developed and deployed the ICE Pattern Analysis and Information Collection System (ICEPIC) for integrating homeland security and LE information, and DHS is in the process of establishing relationships to include other departmental LE agencies' information as well.

SLT agencies have taken similar actions in concert with—and in some cases in advance of—Federal initiatives. Numerous State and major urban areas have adopted local solutions that are now being linked together through common standards and practices. Some of these include Los Angeles, Jacksonville, Eastern Missouri, Washington State, and San Diego. As shown in Figure 1-2, San Diego's Automated Regional Justice Information System (ARJIS) system, which has supported the local sharing environment for many years, is now linked with national information sources.

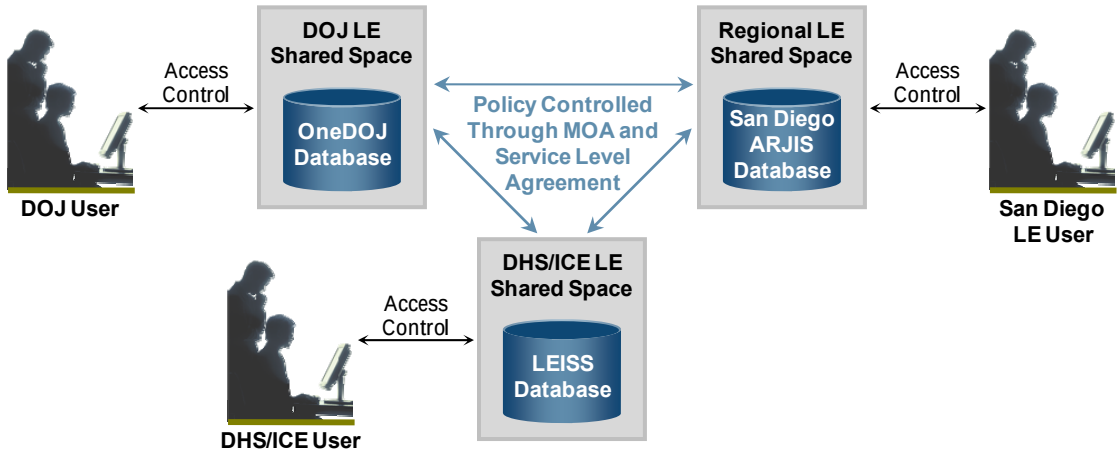


Figure 1-2. Example Law Enforcement Information Flow

With the growing success of these information sharing activities, participating agencies can now search a number of data repositories—commonly referred to as "ISE Shared Spaces"—to assist in connecting activities, trends, or patterns in their jurisdictions to those of others, significantly enhancing intelligence-led policing and terrorism-related crime reduction activities. (See Section 2 for more information on the Shared Space concept.) These efforts all achieve *national sharing* under *local control* and feature distributed architectures, common standards, collaborative governance, improved business processes, and attention to privacy concerns as envisaged and enumerated in the Presidential Guidelines. Further, these efforts leverage, enhance, and extend existing information sharing initiatives, and reflect a shared and growing culture of information sharing on the part of all participating agencies.

1.4 ISE Performance Management

1.4.1 Introduction

Developing the ISE is a continuous, evolutionary process. Effective ISE performance management provides the PM-ISE and the ISC with data to make fact-based decisions and hold agencies accountable for the ISE's evolution. Performance management practices allow the PM-ISE and the ISC to evaluate and refine information sharing policies, business processes, architectures, standards, and systems across all five ISE communities.

Based on the early stage of maturity of many ISE capabilities, performance management activities currently focus on assessing ISE progress. As such, current measures used to gauge ISE implementation progress are characterized as output or compliance measures and generally focus on the progress of individual ISC member agencies. However, as the ISE matures, the performance management approach will itself mature to move from measuring individual agency progress to measuring the overall performance of the ISE. Future measures will evolve, therefore, to emphasize the mission outcomes or results of implementing elements of the ISE. These future measures will focus on the extent to which the ISE has been implemented and sharing improved, while also measuring what has been and remains to be accomplished. This approach will enable the ISE to ultimately measure the performance of its capabilities, including those designated as Fiscal Year (FY) 2009–13 ISE investment priorities. Figure 1-3 depicts the evolution of performance management as it follows ISE maturity.

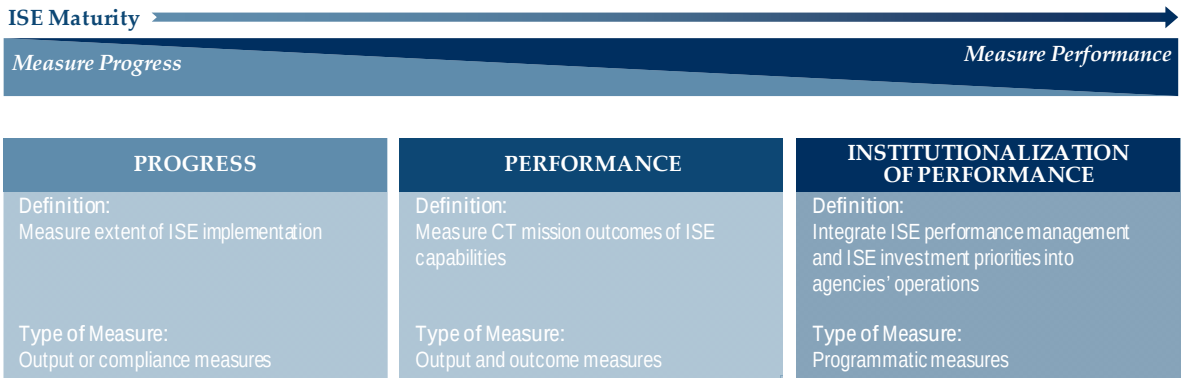


Figure 1-3. ISE Performance Management Evolves as the ISE Matures

Annual performance goals are used to measure the progress in constituting ISE capabilities. First introduced in last year's Annual Report, the four 2008 Performance Goals were designed to provide a target level of performance against which actual achievement could be compared (see Table 1-1). The goals were developed to comply with the performance management requirements of IRTPA, as well as to highlight the direction and strategies embodied in the President's Information Sharing Guidelines and Requirements. The goals are aligned with the Guidelines and Requirements report recommendations that were approved by the President in November 2006, and the data collected from ISC agencies serves to demonstrate that implementation is well underway.

Using these goals and a set of key measurement areas which assess the progress associated with each goal, the PM-ISE and ISC established an ISE baseline of performance in the fall of 2007 and measured agencies' progress against this baseline through an assessment in the spring of 2008. The fall 2007 and spring 2008 performance assessments provided the PM-ISE and the ISC with fact-based data to support decisions and report progress against key information sharing drivers, such as the Presidential Guidelines and Requirements and the NSIS.

Table 1-1. 2008 ISE Performance Goals

2008 ISE Performance Goals
Establish a set of activities and strategic approaches to facilitate sharing among all levels of government, the private sector, and foreign partners.
Develop a shared set of values that change behavior of ISE participants through established training programs, trained personnel, incentive programs, and privacy protections among ISE participants.
Establish interoperability that facilitates sharing through a common ISE Information Technology (IT) security framework, to include approved ISE wide Information Assurance (IA) solutions, government-wide physical and personnel security practices, as well as a Controlled Unclassified Information (CUI) framework across the ISE.
Establish capabilities that allow ISE participants to create and use quality terrorism-related information by improving business processes, developing a common enterprise architecture framework, refining common standards, and instituting effective resource management for government-wide programs.

1.4.2 Performance Assessment Results

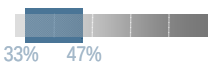
The ISE agencies' self-reported baseline and spring performance data show positive accomplishments across each of the performance goals while highlighting several items that will require further attention as the ISE matures. What the ISC learned from this exercise was that very few agencies had been collecting the data needed to easily track progress against specific ISE initiatives. In addition, most had not yet incorporated meaningful information sharing measures into their own agency performance management processes.

The performance data, gathered from 15 ISC member agencies through the spring and fall assessments, is summarized below. Viewed collectively, the measures demonstrate progress against the 2008 Performance Goals. The gauges next to each measurement area below indicate both the fall baseline and spring levels of performance. As illustrated below, for some of the 2008 Performance Goals, the ISC assessed progress qualitatively but did not establish a specific measure. For these areas, the Report either details the progress made or documents a need for further action to be completed.

2008 Performance Goal: Develop a shared set of values that change behavior of ISE participants through established training programs, trained personnel, incentive programs, and privacy protections among ISE participants.

Roughly half of ISC member agencies reported that they have taken steps to meet this goal of changing behavior in the areas of training programs and personnel, incentives to share, and privacy protections.

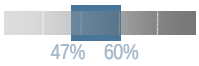
- *Training* – In addition to the ISE Core Awareness Training expected to be available this summer, ISE participants are required to develop tailored training programs that achieve specific, related,



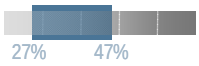
learning objectives.[12] One-third of the agencies surveyed in the fall indicated that they had established and completed some form of training to increase information sharing awareness. This number increased to 47% in the spring assessment and is expected to increase with the publication of the ISE Awareness Training Course in the summer of 2008.

- *Incentives* – Several agencies provided actual examples of how they use incentives to promote information sharing including personnel recognition, cash awards, and other rewards.[13] The overall response of agencies using information sharing incentives grew from 40% last fall to 73% in this spring's performance assessment.

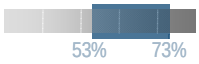
- *Privacy* – Fall baseline data revealed that 47% of agencies had established privacy policies that complied with the ISE privacy guidelines, a number that increased to 60% in the spring assessment. ISE agencies' adoption of the *ISE Privacy and Civil Liberties Implementation Guide,* released in September 2007, is expected to gradually (but significantly) increase the number of privacy-compliant agencies.



- Other Elements of Creating a Culture of Sharing –
  - *Personnel Appraisals* – Last fall, ISE agencies' self-reported data revealed that 27% of ISC member agencies have taken initial steps to ensure accountability for information sharing via performance appraisals. The number grew to 47% this spring, with several agencies requesting coordination with the Office of Personnel Management (OPM) to insert information sharing into their performance appraisals. Additional agencies also reported a desire to use ISE-wide training to determine the elements needed to evaluate personnel performance in terrorism-related information sharing.



  - *Disincentives* – In the fall assessment, 53% of agencies were able to identify steps they took to remove information sharing disincentives in the areas of document dissemination (e.g., reduced use of originator controls), writing for release, and policies for sharing between internal departments. This number increased to 73% for the spring assessment.



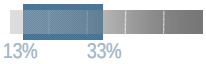
2008 Performance Goal: Establish interoperability that facilitates sharing through a common ISE IT security framework, to include approved ISE-wide Information Assurance (IA) solutions, government-wide physical and personnel security practices, and as a CUI framework across the ISE.

[12] ISE IP, op. cit., p. 84-86.

[13] *Implementing Recommendations of the 9/11 Commission Act of 2007* (9/11 Commission Act), P.L. 110-53, Section 210, (August 3, 2007).

In line with the goal of establishing interoperability, a number of ISC member agencies demonstrated progress establishing ISE shared spaces. However, there is room for improvement in focusing ISE efforts on reducing barriers—both in shared spaces and in physical and personnel security practices as well as in moving toward a CUI framework.

- *Shared Spaces* – The *ISE Profile and Architecture Implementation Strategy (PAIS)* provides the official standard necessary to implement ISE shared spaces was published in May 2008.[14] After close coordination with agency Chief Information Officers (CIOs), enterprise architects, and Office of Management and Budget (OMB) officials, the fall baseline response of 13% of agencies having implemented shared spaces grew to 33% in the spring.



- *CUI Framework* – As noted earlier, a policy framework has been established and released by the President for standardizing SBU (now termed CUI) information. Because the CUI framework was only recently approved (May 2008), the PM-ISE was not able to collect performance data. Section 4 provides further detail on the progress achieved.
- *Physical and Personnel Security Practices* – The ISE has begun to coordinate and collaborate on security policies across the five ISE communities. The PM-ISE did not collect performance data on this topic; however, it intends to focus efforts on this area in the future.

2008 Performance Goal: Establish a set of activities and strategic approaches to facilitate sharing among all levels of government, private sector, and foreign partners.

Considerable progress has been achieved in sharing with Federal and SLT governments, yet further data is needed to evaluate sharing with the private sector and foreign partners.

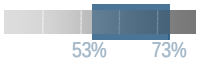
- Sharing Among All Levels of Government –
  - *ITACG* – The Interagency Threat Assessment and Coordination Group (ITACG) has achieved 75% of its initial operating capability, specifically in the areas of staffing, establishing standard procedures, and integrating operations with the National Counterterrorism Center (NCTC).[15]

[14] Version 2.0 of the Enterprise Architecture Framework scheduled to be released in Fall 2008, will provide further detail on ISE Shared Spaces.

[15] For purpose of the Spring 2008 ISE Assessment, initial operating capability was defined as: staffed with the appropriate Federal, state, local, and tribal representatives; operating based on a finalized set of standard operating procedures (SOPs); drafted a budget to be fully funded over the next two fiscal years; reviewing Federal products to ensure that they are incorporating SLT requirements; incorporating the ITACG within DHS and FBI operations; and developing and disseminating products.

Further information on the ITACG can be found in Section 5 of this Report and in a separate Report to Congress.[16]

- *Suspicious Activity Reporting (SAR) Processes* – Roughly half (53%) of agencies reported having a Suspicious Activity Reporting (SAR) process in place. While the data made it clear that SAR processes are generally not yet standard across the ISE, the percentage of agencies that reported having a SAR process in place increased to 73% in the spring assessment.



- *Sharing with Foreign Partners* – The Foreign Government Information Sharing Working Group developed a checklist of issues for agencies to consider when negotiating terrorism-related information sharing agreements with foreign partners, including privacy protections and possible review procedures. Released this spring, the checklist was recommended but not mandatory. As part of the spring 2008 measurement findings, 13% of ISC member agencies reported having adopted the checklist in Department-wide processes.

State and Major Urban Area Fusion Centers - Both DOJ and DHS are able to document Federal activities completed in support of establishing and maintaining a baseline level of capability for fusion centers, including providing training and connectivity, and attempting to tie baseline capabilities to the grants process. Further information regarding fusion centers can be found in Section 3.

Sharing with the Private Sector – Sharing with the private sector is called for in the NSIS and remains a priority for the ISE. Though no performance data were collected at this time, efforts such as the FBI's InfraGard Program which shares information with private sector infrastructure security officials through a homepage on the LEO network, reflect progress achieved in sharing information with the private sector.

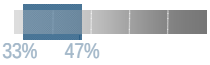
2008 Performance Goal: Establish capabilities that allow ISE participants to create and use quality terrorism information by improving business processes, developing a common enterprise architecture framework, refining common standards, and instituting effective resource management for government-wide programs.

This goal refers to the successful incorporation of information sharing into agencies' routine mission operations. Several elements have been achieved that demonstrate how the ISE agencies are beginning to account for information sharing in their operations, including enterprise architecture, CTISS, performance, and investment structures. These elements will be discussed throughout the remainder of this Report,

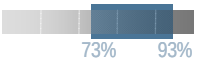
[16] *Report to Congress on Establishing the Interagency Threat Assessment and Coordination Group,* PM-ISE (February 2008). Available online at: http://www.ise.gov.

specifically in Sections 2 and 7. One additional element of ISE institutionalization that was tracked as a part of the baseline and spring measurement efforts was information sharing governance.

- *CTISS* –In part because of their participation in developing the ISE-SAR Functional Standard, the first Common Information Sharing Standards (CTISS) program issuance, 33% of agencies reported adoption of the CTISS Program. The number of agencies adopting the CTISS Program increased to 47% after the January 2008 release of the ISE-SAR Functional Standard, and several agencies were also adopting Agency-wide standards processes. In addition, agencies cited the NIEM and Federal Enterprise Architecture (FEA) Standards as examples of where they are working across the ISE to align technologies to facilitate information access and exchange.



- *Governance* – As a means to facilitate information sharing within their own agencies and across the environment, a full 93% of agencies reported having established their own information sharing governance bodies in the spring assessment. This is an increase from the 73% of agencies that reported having established governance bodies last fall. This measure is a positive indicator of ISE members taking steps to ensure that information sharing is appropriately addressed within their agencies.



ISE accomplishments are clear when viewed according to the Presidential guidelines and requirements. The PM-ISE, in consultation with the ISC, is implementing the guidelines by leveraging ongoing information sharing efforts and promoting a culture of information sharing. The remaining sections of this Report complement the vision for the ISE and the ISE performance management results by providing a detailed overview of ISE progress against each of the Presidential guidelines and requirements, as well as planned activities to further the ISE's evolution in the upcoming year.

2 Establishing Information Sharing Standards

"The ISE must, to the extent possible, be supported by common standards that maximize the acquisition, access, retention, production, use, management, and sharing of terrorism information within the ISE consistent with the protection of intelligence, law enforcement, protective, and military sources, methods, and activities."

— Guidelines and Requirements in Support of the ISE, Guideline 1

A smoothly functioning ISE requires the construction, integration, and sustained operation of standardized terrorism-related information sharing infrastructures across the Federal Government, SLT governments, and where appropriate, the private sector and foreign partners. A business process-driven architectural framework, buttressed by a common standards development approach, is driving ISE architecture and standards implementation by Federal agencies. This section also singles out two areas that are especially important in helping to both help remove impediments to sharing and help agencies improve sharing practices. Implementation of ISE Shared Spaces is discussed in Section 2.4, while the essential ISE attributes of trust and security are covered more fully in Section 2.5.

2.1 2007-08 Highlights

Highlights of progress this year include:

- Publication of the first version of the ISE Enterprise Architecture Framework (ISE EAF) in August 2007 and its companion ISE PAIS in May 2008;
- Formal establishment of the ISE standards program and publication of the first ISE functional standard that institutionalizes an integrated ISE SAR process;
- Development of ISE Shared Spaces to support operational exchanges of terrorism-related information;
- Demonstration of the ISE EAF and CTISS in operational pilots;
- Leveraging of the fundamental concepts of the ISE EAF and PAIS by DOJ, DHS, and others for applications broader than the ISE; and
- Development of a common ISE security risk management framework.

2.2 ISE Enterprise Architecture Framework

A major requirement of the ISE is to standardize and rationalize the inherent differences and distinct separation of information resources across the Federal Government and between Federal and SLT agencies. Systems are budgeted for and implemented by individual agencies in all ISE communities. The challenge then is to provide a unifying

construct—based on common standards and core services—that still accommodates the need for individual ("mostly common") implementations. To address this challenge, the PM-ISE established the ISE Architecture program to align and integrate the vast collection of diverse information technology systems used by all ISE participants into a more uniform, interconnected ISE-wide system of systems. Figure 2-1 depicts a top-level view of a portion of the ISE EAF demonstrating how two ISE participants would share in the ISE.

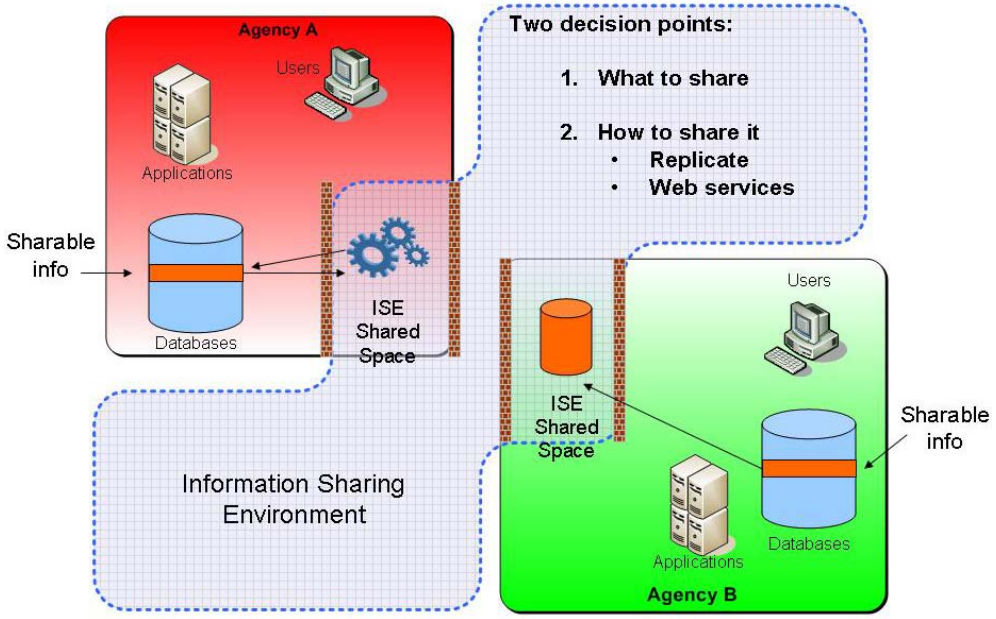


Figure 2-1. Overview of the ISE Enterprise Architecture Framework

The ISE Architecture program, employing cross-governmental working groups such as the Chief Architects' Roundtable, continues to make progress in addressing this technology challenge. Specific accomplishments include:

- In August 2007, the PM-ISE released the first version of the ISE EAF, a strategic guide for mapping ISE participants' enterprise architectures into the Government's FEA. The ISE EAF provides a roadmap to enable long-term, institutionalized technology improvement and information systems planning, investing, and integration to support the sharing of terrorism-related information and identifies the network interfaces and standards needed to facilitate information sharing.
- In May 2008, the PM-ISE released the first PAIS document to help guide ISE Federal agencies with near-term implementation efforts to interconnect information resources; make these resources readily available; and access other data, networks, and services provided by the ISE. The Federal CIO Council's Architecture and Infrastructure Committee and OMB reviewed and approved the PAIS as a valid document to guide information sharing requirements.

2.3 Common Terrorism Information Sharing Standards

The need for ISE standards is cited in thirteen separate places in the NSIS—an explicit recognition that common standards are the fundamental building blocks enabling effective and efficient information sharing. As a result, the PM-ISE has worked with the ISC and SLT governments to develop and implement standards to improve the operation of ISE business processes and implement compatible technology capabilities in ISE participants' networks and supporting infrastructure. The CTISS program integrates information exchange standards, based on common ISE business processes and developed through the DOJ and DHS NIEM program management office, into new ISE-wide functional standards. NIEM epitomizes a successful Federal, State, local, tribal, and private sector initiative and provides a foundation for nationwide information exchanges leveraging data exchange standards efforts successfully implemented by the Global Justice Information Sharing Initiative. NIEM is also being strongly embraced by the private sector technology community. Being part of the ISE EAF and supported by NIEM, the CTISS program is also compliant with the Federal Enterprise Architecture's Data Reference Model, a standards-based model designed to optimize data architectures to help enable information sharing and reuse across federal agencies.

- In October 2007, the PM-ISE formally established the CTISS program. CTISS standards are business process-driven, performance-based "common standards" for preparing terrorism information for maximum distribution and access within the ISE. The CTISS Committee, a subcommittee under the ISC, now provides ongoing governance, configuration management, and cross-agency, cross-government CTISS coordination and review.
- In January 2008, the PM-ISE issued the first CTISS functional standard that provides the data and information sharing foundation for operational information sharing of SARs in the ISE and supports demonstrations to include the SAR Evaluation Environments and an effort by the Los Angeles Police Department (LAPD) to redefine its terrorism SAR policies and processes.
- DOJ and FBI are already working with fusion centers to adopt and implement the SAR functional standard at the Federal level and at selected fusion centers. The Department of State also has a project underway to apply the standard to its SAR database.
- The PM-ISE also identified initial technical standards supporting information assurance and transport to ISE infrastructure assets, and will also actively work with all agencies, including the Department of Defense

In part because of their participation in developing the ISE-SAR Functional Standard, 33% of agencies reported adoption of the CTISS Program. The number of agencies adopting the CTISS Program increased to 47% after the January 2008 release of the ISE-SAR Functional Standard, and several agencies were also adopting agency-wide standards processes.

(DoD), to ensure that standards allow for biometric and biographic information to be maintained in the same intelligence systems.

- In late 2007, PM-ISE, NIEM, and the DoD and Director of National Intelligence (DNI) Universal Core (UCORE) program offices formed a multi-agency partnership for developing new converged information exchange standards supporting the Law Enforcement, Homeland Security, Defense, and Intelligence communities. Plans for the CTISS program in 2008 include incorporating this new multi-community NIEM-UCORE information exchange standard into CTISS as a foundation for developing and implementing new ISE standards. In 2008, NIEM released LEXS defining a common format for law enforcement data for sharing and providing an important linkage between the NIEM-UCORE integration effort and State and local partners.

2.4 ISE Shared Spaces

The term "ISE Shared Spaces"— a key element of the ISE EAF—describes a functional concept, not a technology implementation approach. The ISE EAF helps resolve the information processing and usage problems identified by the 9/11 Commission and IRTPA by employing a structured, networked approach to information sharing. ISE Shared Spaces are networked data and information repositories used by ISE participants to:

- Make standardized terrorism-related information, applications and services accessible to other ISE participants in each of the three ISE security domains—SBU, Secret, and Sensitive Compartmented Information (SCI);
- Deliver an infrastructure that allows ISE participants operating on national security systems (NSS) to exchange information with participants on non-NSS networks; and
- Provide the means for foreign partners to interface and share terrorism information with U.S. counterparts.

Identity management is a fundamental core service of the ISE EAF and essential for controlling access to Shared Spaces. To test potentially useful approaches, the PM-ISE funded a DOJ effort called the trusted broker pilot. In addition to demonstrating important concepts in federated identity management, this pilot also produced operational results, providing the Chicago Police Department access to information that confirmed the identity of suspects and eliminated from consideration those in custody who had been wrongly identified.

Operational examples that demonstrate sharing using the principles of the ISE Shared Spaces implementation approach include:

- The Terrorist Identities Datamart Environment (TIDE), hosted by the NCTC and distributed by the Terrorist Screening Center (TSC), that provides consolidated and validated information on terrorist identities to a wide range of customers;

- NCTC Online, a web-based capability that now allows State and major urban area fusion centers to access Secret national terrorism-related information; and
- Law enforcement information shared by DOJ and ICE, a component of DHS, through LEO and RISSNET.

The PAIS provides the official standard necessary to implement ISE shared spaces. After close coordination with agency CIOs, enterprise architects, and OMB officials, the fall baseline response of 13% of agencies having implemented shared spaces grew to 33% in the spring, as further guidance was made available to agencies.

In these and other cases, the essential point is that such infrastructure elements interconnect and make terrorism-related information accessible to all authorized ISE participants. By FY 2010 agencies participating in the ISE are expected to build on existing or planned information technology resources to create ISE Shared Spaces to support the national CT mission.[17]

2.5 Building a Trusted Environment

The concept of trust is fundamental to the ISE. Seven of the 15 ISE attributes identified in IRTPA deal with aspects of trust or security.[18] The NSIS refers to the terms "trust" or "trusted" at least ten times, calling for the need to "enable the trusted, secure, and appropriate exchange of terrorism-related information … at all levels of security classification." Increased sharing depends on ISE participants' trust that recipient organizations will adequately protect the information against unauthorized disclosure or other misuse. In the last year, Federal agencies have developed a common ISE risk management framework and made strides in improving security practices.

2.5.1 ISE Risk Management Framework

The basis for achieving trust in the ISE is adoption of a common risk management and information security framework to allow officials in all five ISE communities to make the appropriate tradeoffs between sharing and protection and lead eventually to mutual acceptance of security assessments. The risk management framework:

- Embodies the basic principles of information security—confidentiality, integrity, and availability—so that ISE

The FBINET pilot project addresses personnel, facility, and IT requirements for installation of a Secret level capability at a fusion center. In a practical example of risk management, the FBI modified its security requirements which differed from those of DHS to better address fusion centers' needs. More importantly, FBI and DHS are working to harmonize their security requirements for fusion centers so that there will be only one standard for installation and operation of Secret domain networks.

[17] Additional guidance on implementing shared spaces will be provided in Version 2 of the ISE EAF.
[18] IRTPA, as amended, op. cit., §1016(b)(2)(A-O).

participants are assured that the information they provide will be adequately protected;

- Is integrated with the ISE EAF and PAIS; and
- Employs information security standards and guidance developed by the National Institute for Standards and Technology (NIST), and builds on the foundation of trust between the defense and intelligence communities.

Figure 2-2 shows the specific activities in the ISE Risk Management Framework and the NIST security standards and guidelines associated with each activity.

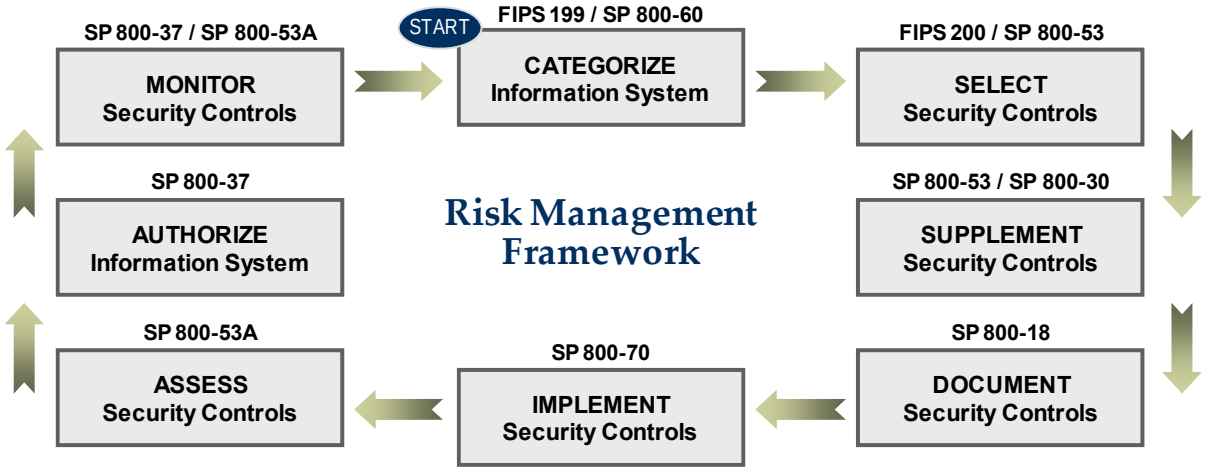


Figure 2-2. The ISE Risk Management Framework

2.5.2 Improved Security Practices

Cumbersome personnel and IT security processes seriously inhibit efficient exchange of terrorist-related information. ISE success ultimately depends on streamlining the granting and mutual recognition of security clearances and IT system accreditations.

- The PM-ISE and ISC are leveraging a joint DoD and DNI CIO effort to drastically streamline the Certification and Accreditation (C&A) process for national security systems. DoD and the Office of the DNI (ODNI) have updated the ISC to ensure that other agencies are aware of the standards and processes they have developed by the ODNI and DoD. The aim is to use using a mostly common set of standards to guide C&A activities across the ISE and achieve reciprocity wherever possible (see the "Authorize block" in Figure 2-2).

The C&A process is used by Federal agencies and others to determine if an information system is approved for operation. Certification involves an evaluation of the technical and non-technical security features of the system. Accreditation is a formal management decision—using certification results as input—that a system is approved to operate at an acceptable level of risk.

- Recommendations for transforming the security clearance process made by an interagency Joint Security and Suitability Reform Team are currently under review. Responding to a February Presidential directive, the team recommends making the clearance process faster, more reliable and reciprocal among all agencies. Planned features include:
  - An automated records-checking system using government and commercial electronic databases to replace some manual investigations;
  - A continuous evaluation program, using frequent automated record checks of cleared employees, to replace the current practice of reinvestigations every five or ten years;
  - A new electronic application that would collect security-related information, including electronic fingerprints, early in the clearance process, reduce errors and speed processing; and
  - Consolidated oversight by the DNI of the security clearance process for all levels of security classification.

2.6 Broader Application of ISE EAF and CTISS

The ISE EAF, PAIS, and CTISS provide guidance to help agencies implement information sharing capabilities, connect to other ISE participants, make information available through ISE Shared Spaces, and access ISE information and services. Because they break new ground in several areas, however, they have had unexpected spin-offs beyond the bounds of the ISE. There are many success stories both inside and outside the ISE resulting from the CTISS effort to leverage NIEM and DoD-DNI UCORE data standards to facilitate information exchanges between different domains or communities of interest.

DHS, for example, is using guidance from the ISE EAF with NIEM to construct almost 50 reusable information exchanges across the full range of its mission areas. The DHS Regional Sharing Service initiative has also deployed information sharing technologies and operating policies in compliance with the ISE EAF supporting information sharing between ICE and local law enforcement agencies in Seattle, WA, Laredo, TX, and Los Angeles, CA. DHS is further using NIEM to develop the next version of the Common Alerting Protocol, a simple, general format for exchanging all-hazard emergency alerts and public warnings over different networks. This capability provides valuable analytic inputs into the ISE-SAR and alerts, warnings, and notifications (AWN) processes with emerging patterns derived from local warnings that might indicate undetected hostile acts. The Domestic Nuclear Detection Office, in coordination with DHS/Customs and Border Patrol, is providing NIEM-based information exchanges with State and local entities, to include those now participating in an interstate radiation detection information sharing effort—the Southeast Transportation Corridor Pilot Program. NIEM is also developing a standard for interoperability between Emergency Operations

Centers in a number of State and local communities that will be an important part of connectivity efforts between collocated fusion centers and the ISE.

DOJ is taking a similar approach, building information sharing segment architectures leveraging concepts from the ISE EAF, with a focus on State and local law enforcement sharing through capabilities such as the N-DEx, supported by LEO, RISS, and the National Law Enforcement Telecommunications System, a state owned system connecting all 50 states and territories along with every federal agency with a Justice component. N-DEx, activated by the FBI in March 2008, currently incorporates data from Oregon, Delaware, Nebraska, and the Oneida Nation with additional SLT participants' information added in the coming months. The PM-ISE is also working closely with the FBI SENTINEL program management office in developing the case management system to be NIEM-conformant to be able to exchange information with ISE systems and processes.

Individual states—including Florida, New York, Texas, and California—are also using NIEM and ISE guidance to drive SAR implementation. The state of Florida is using NIEM for all law enforcement information exchanges between over 453 law enforcement agencies coordinating among eight (seven regional and one State) fusion centers. Fusion Centers in other states are also incorporating NIEM requirements into their information technology procurements, and other ISC member organizations are in varying stages of adopting the same approaches. In one of the more interesting spin-offs, the national health care community is considering leveraging ISE EAF and CTISS concepts to help meet its national health information sharing needs.

2.7 Next Steps

2.7.1 Architecture and Standards

As the PM-ISE and ISC continue to implement terrorism-related information sharing architectures and business process-driven, common standards across the ISE, they must continue to mature the ISE EAF and PAIS and increase the inventory of common standards. Since the role of the PM-ISE is to *plan for and oversee* the implementation of the ISE, actual implementation is the responsibility of Federal agencies. To ensure that this implementation is consistent with the ISE EAF and CTISS, the PM-ISE must leverage the alignment and integration of performance management and investment strategies to institutionalize these infrastructures (see section 7). The primary activity here is to continue to transition architectural guidance and standards back into the Federal Enterprise Architecture. Planned activities include the following:

- Publishing Version 2 of the ISE EAF and ISE PAIS to incorporate additional terrorist watchlist and AWN mission business processes;
- Continuing to identify those processes that will benefit from a functional standard and assigning the necessary resources to develop the business process maps,

information flow descriptions, and data elements that are essential parts of any ISE functional standard;

- Assisting OMB in overseeing implementation of the ISE EAF, Shared Space, and CTISS and related information sharing functional and technical standards through regular reviews of agency Enterprise Architectures and related investment plans;

2.7.2 Building a Trusted ISE

Trust and security will continue to be important considerations for the ISE. 2008-09 plans include:

- Leveraging a joint DoD and DNI CIO effort to streamline departmental C&A processes. Achieve C&A reciprocity between ISC members to the maximum extent possible;
- Aligning policies to guide sharing across multiple security domains by accrediting and deploying at least one solution identified by or developed through the Unified Cross Domain Management Office; and
- Extend the ISE risk management framework to all ISE stakeholders, especially SLT governments and the private sector where appropriate. The PM-ISE and the ISC will build on the ISE Trusted Broker pilot by fielding a limited capability to provide improved access and identity management.

3 Sharing Within, Across, and Between Levels of Government

"Recognizing that the war on terror must be a national effort, State, local, and tribal governments, law enforcement agencies, and the private sector must have the opportunity to participate as full partners in the ISE…"

— Guidelines and Requirements in Support of the ISE, Guideline 2

Combating terrorism is a national mission that requires cooperation at all levels of government and the private sector. The Guideline 2 framework, approved in November 2006, provides the foundation for a variety of activities, described more fully below, that strengthen the ties nationally among agencies with a CT mission.

Critical components of improved sharing are ISE business processes that remove traditional impediments to sharing and streamline the ways in which agencies exchange information. This section outlines progress in critical ISE processes for SAR, terrorist watchlists, and AWN.

3.1 2007-08 Highlights

Highlights of the effort to improve sharing within, across, and between Levels of Government include:

- Establishing the ITACG and initiating development of an integrated network of fusion centers to enable the effective sharing of terrorism-related information between Federal and SLT partners;
- Providing common tools and mechanisms that assist agencies in facilitating the sharing of terrorism information with foreign governments;
- Working with fusion centers and local law enforcement departments to integrate a standard ISE-SAR business process into the day-to-day operational environments of their region; and
- Evaluating terrorist watchlist and AWN business practices to rationalize, standardize, and simplify them within the ISE.

One example of improving sharing practices in the Federal government is the FBI's initiative to equip field agents with personal digital assistants (PDAs) to provide wireless access to a wide range of SBU level terrorist-related information, including watchlists. As the result of a successful pilot effort, the bureau is now deploying 19,500 PDAs to more than 56 field offices.

3.2 Sharing Information with State, Local, and Tribal Governments

As referenced in the NSIS, the national information sharing framework for sharing with SLT governments has two primary objectives:[19]

- Ensuring the Federal Government provides information in ways that better meet the needs of SLT partners through the establishment of an ITACG within the NCTC. This integrated approach allows Federal agencies to work together to disseminate a federally-validated perspective on available threat information.[20]
- Supporting improved collaboration at the State and local levels by designating fusion centers "as the primary focal points within the State and local environment for the receipt and sharing of terrorism-related information" and by establishing and sustaining a national integrated network of these centers.[21]

In July 2007, Congress passed the 9/11 Act which statutorily created the ITACG and designated the PM-ISE "to monitor and assess" its efficacy.[22] The Act also called for a DHS State, Local, and Regional Fusion Center Initiative which, among other requirements, must "support efforts to include State, local, and regional fusion centers into efforts to establish an information sharing environment."[23] The NSIS further advanced these initiatives by providing a detailed description of the role of the ITACG and the roles and responsibilities of Federal and SLT governments. In the past year, significant advances have been made in implementing the NSIS objectives.

3.2.1 The Interagency Threat Assessment and Coordination Group

As required by the 9/11 Act, the PM-ISE submitted a *Report to Congress on Establishing the Interagency Threat Assessment and Coordination Group* which details the progress achieved in establishing the ITACG as of early February. In summary, the ITACG achieved initial operating capability in the areas of staffing, establishing standard procedures, and integrating operations with the NCTC, though more remains to be done before the ITACG can be considered fully operational. Both DOJ and DHS are able to document Federal activities completed in support of establishing and maintaining a baseline level of capability for fusion centers, including providing training and connectivity, and attempting to tie baseline capabilities to the grants process. Since the Report was issued, the ITACG Advisory Council met in April and June 2008, focusing on recruitment for next year's detailees; and agreeing to a Concept of Operations for a Detailee Fellowship Program. The full report is available at www.ise.gov.

---

19 NSIS, op. cit., p. 30.
20 Ibid., p.18.
21 Ibid., p.20.
22 9/11 Commission Act, §521(c), op cit. The ITACG was established as part of the ISE IP and Guideline 2, but the statute strengthened several of its functions and provided for additional oversight.
23 Ibid., § 511(b)(2).

3.2.2 State and Major Urban Area Fusion Centers

Today, there are over 60 operational fusion centers in 48 states. In most states with multiple fusion centers, Governors have designated a single fusion center to coordinate statewide information sharing efforts with the Federal Government. The interagency National Fusion Center Coordination Group (NFCCG), co-chaired by DHS and the FBI, is responsible for ensuring that the Federal Government's efforts to work with fusion centers are coordinated and carried out in a manner consistent with the NSIS.

To further these coordination efforts, the Federal Government is asking that fusion centers achieve and sustain a baseline level of capability and establish electronic connections with the Federal Government and each other. The NSIS goal is an integrated network of fusion centers to enable the effective sharing of terrorism-related information.[24] The Federal Government is developing Baseline Operational Capability Standards for fusion centers to ensure that they have the necessary structures, standards, and tools in place to support the gathering, processing, analysis, and dissemination of terrorism-related information.[25] Once achieved, national baseline capabilities will provide a forum from which fusion centers can support specific operational capabilities such as SAR, AWN, statewide or regional risk assessments, and situational awareness reporting.

Where current Federal support efforts are underway, a sustained Federal partnership with fusion centers is critical. Efforts to build this partnership include:

- *Planning*. A Federal Coordinated Support Plan is under development by DHS, FBI, and other Federal agencies to support the establishment and sustainment of this baseline capability through *technical assistance and training, human support*, and *connectivity*.
- *Technical Assistance and Training*. The DHS/DOJ Fusion Process Technical Assistance Program is assisting fusion centers in achieving baseline capabilities by providing training and technical assistance on such topics as governance, fusion center management, and privacy policy. The Federal Government is supporting an assessment of fusion center

This year, fusion centers provided intelligence used in over 50 DHS Homeland Intelligence Reports (HIR). In March 2008, a DHS HIR from Ohio was used as a source for an article in the Presidential Daily Brief. This is a prime example of how personnel assigned to fusion centers are helping to facilitate the movement of information from state to senior-level Federal authorities.

[24] NSIS, op. cit., pp. 14 and A1-3.

[25] This document is being constructed based on the fusion process capabilities outlined in the 2007 Fusion Center Assessment and the 2007 and 2008 Homeland Security Grant Program Fusion Capability Planning Tool Supplemental Resource. The baseline operational standards are being developed using guidance provided in the following national policy documents: the *Fusion Center Guidelines,* the *National Criminal Intelligence Sharing Plan,* the *Information Sharing Environment Implementation Plan*, and the U.S. Department of Homeland Security's National Preparedness Guidelines and Target Capabilities List.

capabilities, identifying and documenting capability gaps, and developing a strategy and investment plan to mitigate these gaps. Training and technical assistance priorities include improving fusion center analysis and incorporating other disciplines—fire, public health, etc.—into fusion center operations. As of May 2008, 96 technical assistance services had been provided to jurisdictions, and additional technical assistance continues to be available upon request.

- *Human Support*. The Fusion Center Initiative also deploys personnel to assist fusion centers in blending law enforcement and intelligence information analyses and coordinating security measures to reduce threats in local communities. DHS and FBI have deployed over 200 people to fusion centers thus far. This number is expected to grow as part of a coordinated interagency approach that supports the assignment of Federal personnel to fusion centers and strives to integrate and, to the extent practicable, co-locate resources.
- *Connectivity*: Significant progress has been made to provide fusion centers with protected access to Secret and Unclassified Federal systems including direct access to NCTC on line at the Secret level via multiple paths such as FBINET, the DoD Secret Internet Protocol Router Network (SIPRNET), and the Homeland Security Data Network (HSDN). Both DHS and FBI have amended their security policies so that they are consistent across FBINET and HSDN. Access to RISS, LEO, and the Homeland Security Information Network (HSIN) allow users at all fusion centers to communicate and exchange information at the SBU/CUI level. At the Secret level, 16 fusion centers are connected to DHS' HSDN Network and 27 have FBINET connectivity. By the end of 2008, 41 fusion centers will be connected to HSDN and 46 to FBINET.

3.2.3 Tribal Governments

Tribal governments play an important role in our efforts to foster a coordinated SLT information sharing network. In 2006, the ISE and the Department of the Interior initiated the Tribal Nations Information Sharing Pilot Project (TN-ISPP). During 2007, the Project assessed the information sharing needs of four federally recognized tribes whose reservations were located on or near international borders: the Tohono O'odham Nation (Arizona), the Cocopah Tribe (Arizona), the Blackfeet Tribe (Montana), and the Sault Ste. Marie Tribe (Michigan). After the assessments were conducted and prior to TN-ISPP completion in March 2008, equipment was purchased and installed at Blackfeet and Cocopah, which will greatly enhance the ability of those two tribes to better support NSIS requirements. Efforts are also ongoing to explore how best to integrate tribal representation at fusion centers.

3.3 Sharing Information with the Private Sector

As noted in last year's Annual Report, the PM-ISE and ISC agreed in January 2007 to leverage the nation's Critical Infrastructure and Key Resources (CI/KR) sector partnership structure, as defined in the National Infrastructure Protection Plan (NIPP)

and managed through DHS, as the primary private sector coordination mechanism for the ISE. The CI/KR Sector Partnership includes:

- CI/KR owners or operators and trade associations representative of CI/KR owners and/or operators;
- Government agencies and officials relevant to their CI/KR infrastructure protection mission interests; and
- Subject-matter experts upon whom they depend to support infrastructure protection mission activities.

Defined in the NIPP, the partnership includes the 17 CI/KR sectors identified within Homeland Security Presidential Directive 7 (with one additional CI/KR sector created by DHS) along with the cross-sector councils supporting the sector's critical infrastructure protection activities.

DHS is equipping state police flight crews with a cutting-edge aerial technology. Piloted with the Maryland State Police (MSP) Aviation Command, the new technology—known as the Critical Infrastructure Inspection Management System (CIIMS)—helps state police to efficiently manage inspections of critical structures, such as dams, bridges, and large industrial complexes. Before the CIIMS technology was available, MSP flight crews relied upon paper files to document inspections. Nationally replicable, CIIMS provides flight crews with an easy-to-use, tablet-sized computer equipped with touch-screen controls that aid data collection efforts and expedite information sharing among local, State, and Federal agencies.

The CI/KR information sharing environment is being implemented through the development of information sharing policies and the coordinated development of core and enhanced mission-related information sharing processes. It will support three levels of decision-making and action: (1) strategic planning and investment; (2) situational awareness and preparedness; and (3) operational planning and response.[26]

In addition, the FBI InfraGard program is a government and private sector alliance comprised of CI/KR stakeholders from the Federal and SLT governments as well as the private sector. As of February 2008, the number of InfraGard members increased to 24,000 in 86 chapters nationwide. Members have access to InfraGard's secure website on the LEO network infrastructure through which they receive information and CI/KR-related intelligence products at the SBU, Law Enforcement Sensitive (LES), and For Official Use Only levels.

3.4 Improving ISE Business Processes

In this section we describe activities underway to improve and standardize business processes and rules governing suspicious activity reporting; terrorist watch lists; and AWN. The PM-ISE and ISC have been working to define important "to be" business

[26] *The CI/KR Information Sharing Environment*, Department of Homeland Security, Office of Infrastructure Protection (April 2007).

processes to improve the way terrorism-related information is shared and to drive improvements in agency architectures through the ISE EAF and CTISS.

3.4.1 Suspicious Activity Reporting

Law enforcement agencies have long relied on tips and leads about suspicious activity provided by the public and others to support anti-crime efforts. In the post 9/11 world, some of these tips and leads could potentially provide critical information regarding suspicious activities related to terrorist threats. Our challenge is to integrate terrorism-related SARs broadly in the ISE to establish "a unified process to support the reporting, tracking, processing, storage, and retrieval of ... [suspicious activity] information" while ensuring that the effort is carried out in a manner that protects privacy and other legal rights."[27]

This year, the LAPD established a department-wide process for gathering, processing, and sharing terrorism-related SARs. Consistent with the ISE-SAR Functional Standard, this process uses e-learning and roll call training to inform officers how to recognize potential terrorist activities while providing standardized reporting codes that facilitate the reporting and review of terrorism related suspicious incidents. LAPD is blending suspicious activity reports with other critical infrastructure and relevant crime data in order to identify patterns and trends that may be indicators of potential threats to locations within the city. LAPD SARs will be shared with analysts at the Joint Regional Intelligence Center and blended with information from other jurisdictions so that patterns and trends can be evaluated on a regional basis. DOJ and the Major Cities Chiefs Association are working together to use the LAPD process as a model that can be replicated in other cities.

Building on the foundational work and top level ISE-SAR business process description completed last year, there is substantial progress toward achieving this goal. The ISE-SAR Functional Standard, issued by the PM-ISE in January 2008:

- Requires all departments or agencies that possess or use terrorism or homeland security information or operate systems that support or interface with the ISE to follow a common format for sharing SAR information;
- Outlines a set of general criteria to assist operators or analysts in determining whether or not a particular report meets the threshold for designation as an ISE-SAR, i.e., one with a potential terrorism nexus; and

Roughly half (53%) of agencies reported having a SAR process in place. While the data shows that SAR processes are not yet standard across the ISE, the percentage of agencies that reported having a SAR process in place increased to 73% in the spring assessment

[27] NSIS, op. cit., (October 2007), pp. A1-6 and A1-7.

- Describes the ISE-SAR information flow, highlighting the filtering and decision-making steps that separate terrorism-related SARs from the large volume of unrelated information.

As called for in the NSIS, and building on the ISE-SAR functional standard, efforts are underway to pilot and establish a national capacity for gathering, documenting, processing, analyzing and sharing terrorism related SARs.

As an initial step, the DOJ, DHS, DoD, and the FBI, working in partnership with State and local officials, will institute a standardized approach to gathering, documenting, processing, analyzing and sharing terrorism-related suspicious activities reports. Front line law enforcement personnel will be trained to recognize behaviors and incidents indicative of criminal activity associated with domestic and international terrorism. Once documented, SARs will be evaluated by trained personnel to determine if they have a terrorism nexus. If a terrorism nexus is established, the SAR will be made available to the local JTTF, regional and/or statewide fusion centers, and DHS.

Technical resources are being provided to enable the "posting" of terrorism-related SARs to a "shared space" in a manner consistent with technical standards contained within the *ISE SAR Functional Standard* and its associated SAR Information Exchange Package Document. This will allow SARs to be accessed by fusion centers, DHS Headquarters, and JTTFs to support regional and/or national analysis. Access to the "shared spaces" will be via LEO, RISSNET and HSIN.

Protecting the information privacy and legal rights of Americans is a top priority: At the local level, SARs will be incorporated into existing processes and systems used to manage other crime-related information and criminal intelligence so as to leverage existing policies and protocols utilized to protect the information privacy, civil liberties, and other legal rights of the general public. Multiple levels of review and vetting will be established to ensure that information is legally gathered and managed, and reports containing personally identifiable information that are unfounded, or that cannot be reasonably associated with criminal activity, will not be shared beyond the originating entity.

The ISE Privacy Guidelines Committee's (PGC's) Legal Issues Working Group has completed an initial privacy and civil liberties review of the *ISE SAR Functional Standard* and its implementation. The PGC will monitor this effort, provide advice and guidance to the project teams, and issue a public report regarding privacy and civil liberties issues pertaining to this effort.

The results of this initial phase of the ISE SAR pilot will be documented to support the development and publication of an implementation guide and template for use by other state and local jurisdictions. The International Association of Chiefs of Police (IACP), the Major Cities Police Chiefs Association, Major County Sheriffs, and the Criminal Intelligence Coordinating Council (CICC) have been involved in planning and will be major players in implementation.

3.4.2 Terrorist Watch Lists

One of the most important weapons in the fight against terrorism is the U.S. Government's consolidated terrorist watchlist—the authoritative source for information on all known and appropriately suspected terrorists. The list is used by Federal and SLT agencies—including officers on the street—as well as selected foreign and private sector partners to identify and screen terrorists. An accurate terrorist watchlist, shared across the ISE, contributes both to safeguarding our nation's borders and controlling terrorist movements within the country.

The TSC has taken important steps to ensure that watchlists are accurate, standardized, and complete and that appropriate processes are in place to address Congressional direction that "all terrorism watch lists are available for combined searching in real time through the ISE and [that] there are consistent standards for placing individuals on, and removing individuals from, the watch lists, including the availability of processes for correcting errors."[28] Most recently, the TSC has:

- Established a proactive mechanism—the Terrorist Encounter Review Process—to review watchlist data related to frequently encountered individuals and make corrections or enhancements to the watchlist as appropriate;
- Expanded its efforts to ensure the quality of watchlist data by increasing the number of staff assigned to data quality management and improving quality assurance processes;
- Performed selected scrubs of watchlist data, including a special quality assurance review of the No Fly List and an ongoing record-by-record review of the entire Terrorist Screening Database (TSDB);
- Established a process and a separate office to address complaints filed by persons seeking relief from adverse effects of related terrorist watchlist screening;
- Established an interagency working group to review and implement watchlist improvement opportunities; and
- Reached out to State and major urban area fusion centers and Joint Terrorism Task Forces to help them better understand the role of the TSC and use the TSDB more effectively.

Building on TSC existing business processes, the PM-ISE is currently identifying any significant watchlist screening and information sharing gaps with implications for the ISE and making recommendations for updates to those processes as appropriate. To date, the team has:

[28] IRTPA as amended, op. cit., §1016(h)(2)(E).

- Developed a high-level, unclassified end-to-end business process and information flow from terrorist watch list nomination through the identification of information in the TSDB;
- Documented information flows for critical sub-processes including *Nomination* (includes export), *Encounter Management* (includes screening), *Redress* (includes updates to TSDB), and *General Quality Assurance*;
- Identified opportunities for improved use of the terrorist watchlist process in the ISE, to include possible development of an ISE functional standard; and
- In partnership with the TSC, DHS and NCTC worked to determine areas for improved alignment between the ISE-SAR Functional Standard and the Terrorist Watchlist Personal Data Exchange Standard (TWPDES 1.2b) in support of the *Encounter Management* process.

3.4.3 Terrorism-Related Alerts, Warnings, and Notifications

The ability of participants to generate, disseminate, and receive AWNs of potential or impending terrorist activities in near-real time is a fundamental ISE capability. The NSIS requires that the Federal Government, in coordination with SLT partners, establish processes to manage the issuance of AWNs to fusion centers regarding time sensitive threats and other information requiring some type of State or local response.[29]

Terrorist-related AWNs are produced by agencies at all levels of government—some in response to explicit statutory or regulatory requirements. They take several forms and may be disseminated through different distribution channels. Unlike the case with SAR, where the national strategic direction was to establish a unified ISE-SAR process, the situation with AWN is more complex. The goal is to rationalize, standardize, and simplify the multiple existing AWN processes that are either part of the ISE or interface with the environment in some way. As a first step, the PM-ISE and the ISC have been working to better understand the multiple "as is" processes before developing the longer term vision of how the ISE AWN process should operate. The following is the current status:

- There is general agreement on an initial working definition for AWN and development is underway of a top level analysis of the existing AWN business processes and information flows focusing on the key Federal AWN producers;
- There is now baseline information from ISC members concerning terrorism-related AWNs they produce or receive; and
- Preliminary descriptions exist for how two of the primary ISE AWN producers—NCTC and DHS—currently develop and disseminate AWN information.

[29] NSIS, op. cit., p. A1-7. The NSIS discusses AWN separate from what it refers to as "Situational Awareness Reporting," but since the same policies, processes, and applied technologies support both capabilities, we consider the two to be part of one ISE business process.

3.5 Terrorist-Related WMD Information in the ISE

The 9/11 Act amended the definition of "terrorism information" in Section 1016 of IRTPA to specifically include weapons of mass destruction (WMD) information "that could be used by a terrorist or a terrorist organization against the United States." The PM-ISE, in coordination with the ISC and with Intelligence Community (IC) and non-IC partners, has begun to document how terrorist-related WMD information is incorporated into the ISE by examining information flows across the Federal Government and from the Federal Government to SLT partners. The aim is to build upon ongoing efforts to improve the sharing of terrorist-related WMD (WMD-T) information. These efforts provide a solid foundation for improved sharing within (and outside) the WMD Community. Initiatives, to be developed in collaboration with the existing WMD information sharing community, include:

- Establishment of electronic communities of interest that provide the counterproliferation (CP) and CT communities with a common electronic workspace to address WMD-T and the CP-CT nexus issues;
- Coordination between members of the IC and non-IC partners (e.g., Inter-and Intra-agency steering, coordination, and working groups) on issues related to CP, WMD-T and the CP-CT nexus; and
- Production of tri-seal WMD terrorism threat briefings by DHS, FBI, and NCTC to ensure that SLT partners receive coordinated, accurate WMD information regardless of the source.

3.6 Next Steps

Information sharing will continue to mature as strong partnerships with Federal agencies, SLT authorities, private sector organizations, and foreign partners and allies are established and enhanced.

3.6.1 Sharing Information with SLT Governments and the Private Sector

Moving forward, the Federal Government will meet the needs of SLT partners by disseminating a federally-validated perspective on available threat information through the ITACG/NCTC and by supporting the establishment and sustainment of a national integrated network of fusion centers. Planned activities include the following:

- A fully-functional ITACG with increasing impact; and
- An approach to ensure the achievement and sustainment of a baseline-level of capability at designated State and major urban area fusion centers through:
  - Developing and maintaining a Coordinated Federal Support Plan that describes Federal Government-provided technical assistance and training, personnel support, and connectivity to State and major urban area fusion centers.

- Ensuring that, by the end of 2009, all designated statewide fusion centers that can support Secret-domain information systems have appropriate access to Secret and unclassified Federal systems that share terrorism-related information, to include direct access to NCTC on line via multiple paths including FBINET, SIPRNET, and HSDN.
- Developing a national investment strategy to sustain fusion center operations, including a delineation of current and recommended future Federal and non-Federal costs.

3.6.2 Suspicious Activity Reporting

The issuance of the ISE-SAR Functional Standard provides a solid foundation on which to build a national SAR process. Planned activities include the following:

- Revising the ISE-SAR Functional Standard and selection criteria as necessary, based on results analyzed from the ISE-SAR evaluation environments;
- Identifying and implementing lessons learned at the Federal, SLT levels from the SAR evaluation environments and replicate best practices, as appropriate;
- Periodically assessing the ISE-SAR Functional Standard and make adjustments as necessary to ensure that privacy rights are rigorously guarded; and
- Monitoring Federal agencies as they take the steps necessary to implement the ISE-SAR Functional Standard, including resource allocation adjustments where necessary.

3.6.3 Terrorist Watchlists

As with any process, attaining continuous improvement will require a broad and deep understanding of the terrorist watchlist processes involved, stakeholder needs, capabilities and limitations of technology, and collaboration and coordination among all parties involved. In the next year, the TSC will:

- Improve the accuracy and completeness of the terrorist watchlisting process; and
- Provide accurate and timely information from the TSC to all screening agencies.

3.6.4 Alerts, Warnings, and Notifications

Work is under way to ensure that all appropriate Federal entities with a potential role in AWN have been identified and to determine any outstanding Federal, SLT AWN needs. In the next year, the PM-ISE and the ISC will rationalize, standardize, and simplify the ways AWNs are handled in the ISC by:

- Identifying issues and impediments to the efficient and effective flow of terrorism-related AWN information between the Federal and SLT governments and the

private sector. This work will also include identification of the types of AWN information products SLT governments require and preferred formats and delivery methods; and

- Completing a baseline categorization of existing terrorism-related AWN information flows. Once this baseline is complete, develop an approach and actions to close identified gaps.

3.6.5 Terrorist-Related WMD Information

ISC agencies will collectively evaluate existing WMD information sharing flows within and among their agencies to determine the effectiveness of current processes and identify and resolve gaps in the WMD-T information sharing processes to facilitate the full incorporation of WMD-T information into the ISE.

4 Standardizing Procedures for Sensitive But Unclassified Information

"To promote and enhance the effective and efficient acquisition, access, retention, production, use, management, and sharing of Sensitive But Unclassified (SBU) information, including homeland security information, law enforcement information, and terrorism information, procedures and standards for designating, marking, and handling SBU information (collectively…must be standardized across the Federal Government."

— Guidelines and Requirements in Support of the ISE, Guideline 3

Providing an effective and efficient process for marking, handling, and sharing SBU information securely is an essential requirement for the ISE.[30] SAR information, for example, only rarely is classified. But it is critical that SARs be clearly marked and exchanged only over networks that provide adequate protection against loss or unauthorized disclosure. There are two separate but related ISE initiatives in this area:

- Establishing a streamlined framework that rationalizes the policies and processes for marking and handling SBU information; and
- Ensuring that systems that process, store, or share SBU information take adequate measures to prevent it's loss or unauthorized disclosure.

4.1 2007-08 Progress

4.1.1 Standardizing Procedures for Sensitive But Unclassified Information

SBU information is currently shared according to an ungoverned body of policies and practices that confuse both its producers and users. Across the Federal Government today more than 100 unique markings and over 130 different labeling or handling processes and procedures are used for SBU information. The result is an unmanageable collection of SBU sharing practices that impede the proper flow of information between Federal, SLT, and private sector partners. This is a national concern because the terrorist threat to the nation requires that many communities of interest, at different levels of government, share this vital but sensitive information.

[30] Although the President's approval of the new CUI framework means that, for the ISE, all SBU information is now CUI, in this Report we continue to use the terms interchangeably because of the deep historical roots of the term "SBU." Over time, however, the term CUI will replace SBU.

The new CUI framework:

- Creates a single policy for the government, reducing over 100 different SBU markings to three:
  - Standard Safeguarding and standard Dissemination;
  - Standard Safeguarding and specified Dissemination; and
  - Enhanced Safeguarding and Specified Dissemination.
- Describes the mandatory standards for the designating, marking, safeguarding, and disseminating of all controlled unclassified terrorism-related information originated by the Federal Government and shared within the ISE, regardless of the medium used for its display, storage, or transmittal;[31] and
- Strongly encourages its adoption by SLT and private sector entities.

Once fully implemented, this Framework will:

- End confusion about proper access, handling, and control of unclassified information that needs protection;
- Instill confidence that identical rules apply to everyone using the CUI markings; and
- Provide clear guidance to SLT partners now confused by SBU markings.

On May 9, 2008, the President issued a memorandum requiring agencies to implement the CUI framework. In addition, the President designated the National Archives and Records Administration (NARA) as the Executive Agent. NARA, in coordination with a CUI Council, will govern the new Framework and oversee its implementation.

An example of Confusion:

Ten different Federal agencies use the marking "LES" for Law Enforcement Sensitive information; however, the term is not uniformly defined across these ten agencies nor are there common rules governing access to "law enforcement sensitive" information. Consequently, each agency decides how to control and to whom to disseminate LES. An individual can have access to LES information in one agency but be denied access in another.

4.1.2 Protected SBU Transport

The PM-ISE, at the request of ISC members, established an interagency working group to better understand the continuing proliferation of unclassified ISE networks and develop recommendations for a more coherent approach. The working group analyzed and documented the current SBU environment in an effort to better understand and

[31] There are certain important infrastructure protection agreements between the Federal Government and the private sector that, because of additional safeguarding requirements are not fully accommodated under the proposed CUI framework. As a result, these Federal regulations with their associated markings, safeguarding requirements, and dissemination limitations will be "grandfathered" into the CUI framework.

define the process, policy, and technology issues with sharing SBU information. The group's recommendations prioritized the need for protected unclassified connectivity among all ISE participants and the need for an "information attribute" based identity management solution. In summary, the group concluded that:

- The ability to share SBU information across the ISE is less robust than it should be because of a variety of factors including limitations on protected interconnectivity between agencies, adequacy of and accessibility to agency-level shared space, proliferation of user accounts, and lack of enterprise-level access control and identity management services; and
- Agencies do not always use protected email services or networks to transport email containing SBU.

After reviewing Working Group findings, a majority of ISC members concluded that, although there are existing capabilities that can be exploited immediately to remedy some of these issues at minimal cost, there are no unaddressed Federal level mission imperatives that demand resolution of SBU connectivity and improvements to information sharing at the SBU level today.

4.2 Next Steps

4.2.1 Implementing the CUI Framework

The first step is to stand-up the CUI Executive Agent and the CUI Council. After initial stand-up is complete, the CUI Executive Agent, NARA, in coordination with the CUI Council, will manage and oversee the implementation of the CUI framework.

4.2.2 Protected Transport

It is imperative that Federal agencies protect the confidentiality, integrity, and availability of information stored, processed, and transmitted on SBU systems and ensure the authentication of access to such systems, as required. At the State and local level, challenges exist with managing multiple, competing, or duplicative information systems; redundant information from multiple systems; and limited ability to receive and share information with those who need it.[32] Planned activities include:

- Taking appropriate measures in support of U.S. policy, strategy, guidelines, and implementation actions to secure cyberspace, taking appropriate measures to reduce the risk to terrorism-related SBU systems and information stored on these systems and adequately deter, reduce, and limit the loss of information or the operational degradation of information systems critical to the ISE; and

[32] *Federal Efforts Are Helping to Address Some Challenges Faced by State and Local Fusion Centers* (GAO-08-636T), (April 17, 2006).

- Working with the ISC State and Local Subcommittee to determine those SBU network and service improvements that State and local partners view as important and the implementation priorities they deem appropriate. Based on insights gained, and leveraging the knowledge from the FY 2008 ISE SBU Network systems assessment, the activity will focus on the Law Enforcement and Homeland Security communities, leading to improved connectivity between agencies at all levels.

5 Sharing with Foreign Partners

"The ISE must support and facilitate appropriate terrorism information sharing between executive departments and agencies and foreign partners and allies."
— Guidelines and Requirements in Support of the ISE, Guideline 4

Recommendations in the Presidential Guideline 4 Report, as well as the NSIS, recognize that the "effective and substantial cooperation with our foreign partners requires sustained liaison efforts, timeliness, flexibility, and the mutually beneficial exchange of many forms of terrorism-related information."[33] The ISE fosters this cooperation by providing a community of interest in which ISC member agencies can collaborate on the bi-directional sharing of terrorism-related information with foreign partners, including the identification of best practices for negotiating foreign sharing agreements and development of standards for safeguarding and handling foreign government information.

5.1 2007-08 Progress

Formally established in March 2008, the interagency Foreign Partner Information Sharing Coordinating Committee, co-chaired by State and the PM-ISE, develops and provides tools and mechanisms that assist agencies in facilitating the sharing of terrorism information with foreign governments. 2007-08 progress in developing these tools includes:

- Issuance of the *Checklist of Issues for Negotiating Terrorism Information Sharing Agreements and Arrangements* to assist in the standardization of terrorism-related information sharing best practices by detailing internal U.S. Government considerations (including considerations around privacy information), considerations specific to the agreement or arrangement, and sources to consult during the agreement development and negotiation process.[34] As part of the spring 2008 measurement findings, two ISC member agencies reported having adopted the checklist in Department-wide processes.
- Stand-up of *a Repository of Foreign Sharing Agreements,* to allow ISE participants to identify and analyze existing, unclassified foreign agreements. Hosted on HSDN, and currently in the user acceptance test phase, the repository provides a user-friendly interface that allows agencies to access and review metadata and/or full text agreements.

[33] NSIS, op. cit., p. 26.
[34] *Checklist of Issues for Negotiating Terrorism Information Sharing Agreements* (ISE-G-101), PM-ISE (March 2008).

Furthermore, the NSIS rightly recognizes that the protection of privacy and civil liberties is essential to the successful sharing of information with our foreign partners. The U.S. is currently in negotiations with the European Union (EU) to develop a set of common principles for privacy and data protection for the information exchange between the U.S. and the EU. Although these principles are specific to the EU, the lessons learned, as well as the principles themselves, will also be applicable to other areas and regions that are partnering with the U.S. on the exchange of terrorism-related information.

5.2 Next Steps

Planned activities include the following:

- Continuing to identify government-wide best practices regarding internal procedures for expediting disclosure decisions and common standards or protocols for electronic handling of foreign government information in the ISE;
- Encouraging broad usage of the *Checklist of Issues for Negotiating Terrorism Information Sharing Agreements and Arrangements* to agencies responsible for the negotiation of foreign agreements and arrangements with foreign partners;
- Evaluating opportunities and, where appropriate, developing common foreign information sharing standards or protocols for the electronic handling of foreign government information within the ISE;
- Evaluating opportunities and, where appropriate, enhancing the *Repository of Foreign Sharing Agreements* to potentially include information on planned or ongoing negotiation activities;
- Determining how the U.S./EU privacy principles apply to the requirements of the Privacy Guidelines to ensure consistency in privacy standards across ISE member agencies and in negotiations with our foreign partners; and
- Ensuring that agency Privacy Act systems of records notices and routine use guidance provides for terrorism information sharing with foreign partners.

6 Protecting Privacy & Other Legal Rights

"[T]he Federal Government has a solemn obligation, and must continue fully, to protect the legal rights of all Americans in the effective performance of national security and homeland security functions."

— Guidelines and Requirements in Support of the ISE, Guideline 5

6.1 2007-08 Progress

Progress in protecting information privacy and civil liberties in the ISE is fundamental to creating a culture of information sharing. The ISE Privacy Guidelines create a uniform framework to help Federal agencies balance the dual imperatives of sharing information and protecting privacy by establishing uniform procedures for implementing required protections in specific legal and mission environments. The ISE PGC, with significant input from State and local members of the Global Justice Information Sharing Initiative (Global), has addressed issues relating to privacy guidance and facilitates, in consultation with the Privacy and Civil Liberties Oversight Board, the implementation of the Privacy Guidelines in ISE participant organizations. The PGC also periodically consults with civil liberties, privacy, and open government advocacy groups.

Over the course of the last year, the PGC has developed tools and resources to assist these agencies in identifying and resolving privacy and civil liberty related issues. Its efforts include the following accomplishments:

Fall baseline data revealed that 47% of agencies had established privacy policies that complied with the ISE privacy guidelines, a number that increased to 60% in the spring assessment. ISE agencies' adoption of the ISE Privacy and Civil Liberties Implementation Guide is expected to gradually (but significantly) increase the number of privacy-compliant agencies.

- Developed and released the *Privacy and Civil Liberties Implementation Guide* to help Federal agencies implement the *Privacy Guidelines;*[35]
- Developed the *Privacy Guidelines Implementation Manual* to serve as a single, comprehensive, resource to assist Federal Agencies in this process;

[35] The *ISE Privacy and Civil Liberties Implementation Guide* (September 2007) helps Federal agencies implement the ISE Privacy Guidelines. This Guide describes best practices and a methodology to ensure implementation of the protections and safeguards required by the *ISE Privacy Guidelines*. Available online at: http://www.ise.gov/pages/privacy-implementing.html.

- Finalized a series of *Key Issue Guidance* papers providing guidance and possible methods or "best practices" on such topics as redress, notice mechanisms, data quality, data security, accountability, enforcement, and audit; and
- Provided ongoing resources to house ISE Privacy Guidelines-related documentation at http://www.ise.gov/pages/privacy-implementing.html

DOJ's Bureau of Justice Assistance (BJA) and DHS—the two primary Federal grant making agencies that fund activities to assist SLT criminal justice and public safety programs—propose to insert a special condition in appropriate new or supplemental award documents requiring compliance with Section 11 of the ISE Privacy Guidelines. BJA is also exploring solicitation language that encourages SLT agencies to adopt privacy policies and procedures that are at least as comprehensive as those contained in the ISE Privacy Guidelines.

6.2 Next Steps

The work of the PGC over the last year has laid a strong foundation for continuing efforts to protect privacy and civil liberties in the ISE. In 2008-09, the PM-ISE and ISC will work with all appropriate parties to identify current information sharing policies, assess if current policies meet ISE implementation requirements, and protect privacy and civil liberties by developing ISE privacy policy to complete Stage 1 of the *ISE Privacy and Civil Liberties Implementation Manual*. The effort to develop and assess a unified SAR process will be a primary driver for these activities.

7 Leveraging Ongoing Information Sharing Efforts

"The ISE shall build upon existing Federal Government policies, standards, procedures, programs, systems, and architectures...used for the sharing and integration of and access to terrorism information, and shall leverage those resources to the maximum extent practicable..."

— Guidelines and Requirements in Support of the ISE, Requirement 1

Although the PM-ISE, in consultation with the ISC, will continue to guide and oversee ISE implementation, as the ISE matures, agencies are ultimately responsible for implementation. Accordingly, they must take greater ownership of targeted outcomes, and be accountable for success as set forth in the agreed upon performance goals and measures. Leveraging ongoing information sharing efforts is an important element of the ISE. Other sections of this report include examples of initiatives that have served as building blocks for broader information sharing efforts. Highlights include:

- FBI-sponsored JTTFs combine Federal-State-Local units dedicated to combating terrorism in specific geographical areas.
- State and major urban area information fusion centers work closely with JTTFs and other Federal partners, and are dedicated to protecting our communities from all-crimes and all-hazards.
- Federal, SLT, and private sector governance structures such as the Federal CIO Council, the Global Justice Information Sharing Initiative, and the National Infrastructure Protection Plan sector partnership model, provide subject matter expertise and contribute directly to the development of ISE capabilities.
- The ISE EAF provides a common architectural structure for agencies to use to incorporate their information sharing capabilities into the ISE. ISC members, including DHS and DOJ, are adopting this architectural framework to enable their ISE participation. In addition, because it breaks new ground in several areas, others—notably the national health care communities—are now leveraging ISE EAF concepts to help develop Information Sharing Segment Architectures to interface not only with the ISE but also with other missions supported throughout their communities.
- The CTISS program incorporates information exchange standards developed by DOJ's and DHS's NIEM program office as part of new ISE-wide functional standards. The first of these addresses the high priority NSIS requirement for a unified process for gathering, documenting, processing, analyzing, and sharing SAR information. In late 2007, PM-ISE, NIEM, and the DoD and DNI UCORE program offices formed a multi-agency partnership for developing new converged

information exchange standards supporting the Law Enforcement, Homeland Security, Defense, and Intelligence communities.

- The DoD-DNI Cross-Domain Management Office, an interagency initiative that is identifying solutions for exchanging information among different security classification levels and domains and ensuring a core group of cross domain solutions is available for use by both the defense and intelligence communities.

In addition to the examples above, there are two primary institutional enablers that allow for effective leveraging of ongoing agency efforts—successful ISE governance and a well-structured investment process.

7.1 ISE Governance

The overall governance of the ISE is described in Chapter 4 of the ISE Implementation Plan. This structure has worked well and will continue to provide top-level direction in accordance with IRTPA and the NSIS. In addition, the PM-ISE and the ISC have established a number of subordinate bodies to guide specific aspects of ISE implementation. These include:

- *The Senior Level Interagency Advisory Group* (SLIAG) that monitors and oversees implementation of the Guideline 2 recommendations;
- *The CTISS Committee* that identifies and recommends common standards for issuance by the PM-ISE, evaluates impacts and potential incompatibility issues with other Federal Government standards programs, and monitors CTISS implementation; and
- *The ISE-SAR Steering Committee* with membership from Federal agencies and SLT organizations who play leading roles in the development and maturation of the nationwide ISE SAR process.

As a means of facilitating information sharing within their own agencies and across the environment, 93% of agencies reported having established their own information sharing governance bodies. This measure is a positive indicator of ISE members taking steps to ensure that information sharing is appropriately addressed within their agencies.

Although this section highlights the interagency governance efforts, individual agencies are also establishing governance processes and institutions to make information sharing an integral part of their internal policy and business process structure. The DNI, for example, established the IC Information Sharing Office of Facilitation and Resolution in November 2007 to improve information sharing throughout the Intelligence Community and to serve as the single point of entry for the resolution of information sharing issues. If a case cannot be resolved, either party to the case may request referral to the DNI for a final decision. Other existing Federal and SLT governance structures such as the Federal CIO Council and the Global Justice Information Sharing Initiative (Global) provide subject matter expertise and input in the development of ISE capabilities

7.2 ISE Investment Planning

7.2.1 The ISE Planning Cycle

Investment oversight and planning are important parts of managing the ISE. Coordinated, cross-ISE investment planning provides insight into ISC members' programs and budgets and will help ensure that ISC member agencies include ISE initiatives in their out-year planning and investment efforts. Over the past year, the PM-ISE has assessed the costs associated with ISE priorities, and more importantly, forged close strategic partnerships with OMB and the NCTC Directorate of Strategic Operational Planning, resulting in issuance of coordinated budget guidance for ISE agencies and establishment of a repeatable investment management process through the *ISE Planning Cycle*.[36]

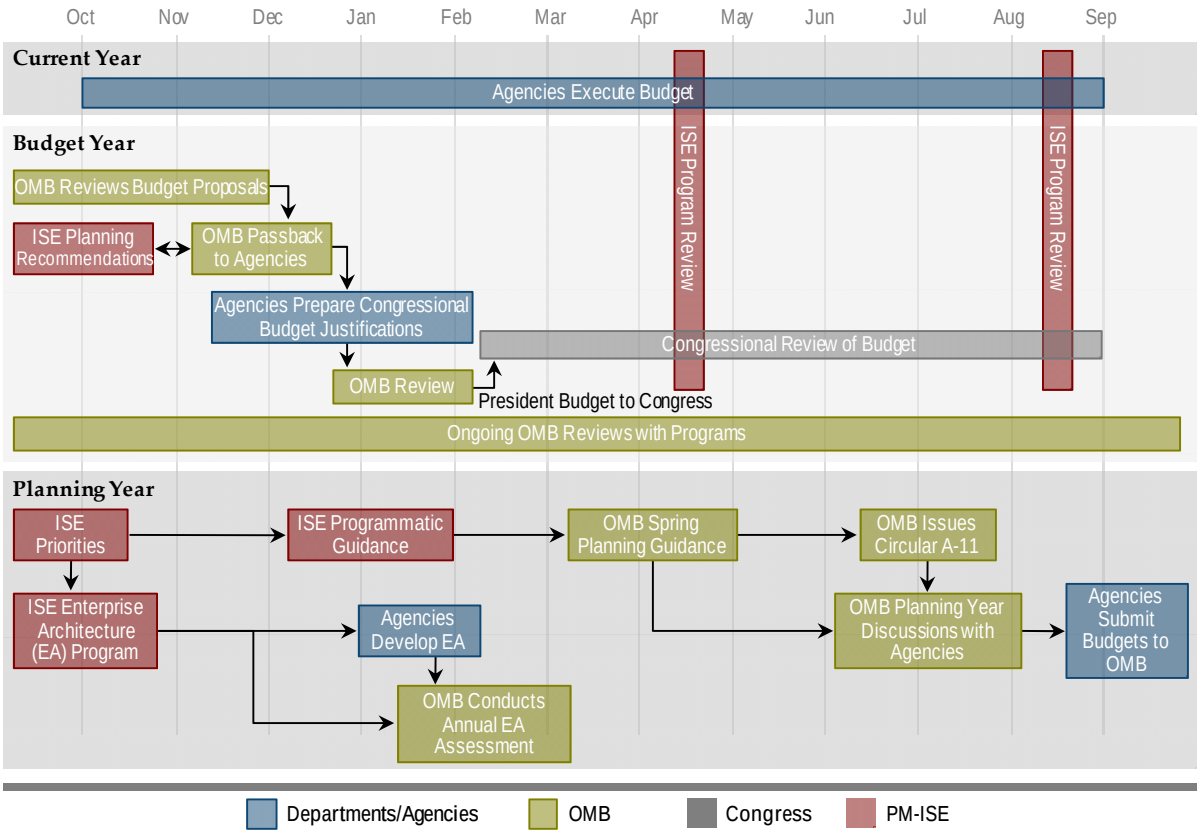


Figure 7-1. ISE Annual Planning Cycle

[36] The ISE Planning Cycle will further help "to ensure that procurement of and investment in systems and technology" are consistent with the direction of the ISE as required by IRTPA §1016(h)(2)(D).

The *Cycle* coordinates the ISE's strategic direction, resource planning, and program oversight. It is based on supporting OMB's existing processes and procedures and includes the steps involved in planning, programming, budgeting, and executing the resources necessary to institutionalize the ISE. Going forward, this Cycle (Figure 7-1) will help better coordinate the ISE's strategic direction, resource planning, and program oversight responsibilities.

7.2.2 Assessing Costs for ISE Priorities

Because ISE resources often account for only a small percentage of larger agency initiatives and are difficult to identify separately, the focus of ISE investment assessment efforts has been on costs associated with planning for and implementing specific ISE priorities. The PM-ISE developed such an assessment related to ISE-specific initiatives for FY 2007, providing an initial point of reference for future planning and budgeting. This effort created a foundation to better understand ISE expenditures and planned budgets addressing the intent of IRTPA to provide insight into the costs of developing and maintaining the ISE.[37]

Recognizing the challenge in separating out information sharing from larger mission operations costs, the effort focused on the costs associated with a limited subset of ISE priorities—those initiatives requiring a commitment of resources that would implement Congressional mandates and the President's priorities as outlined in the NSIS. For the FY 2009–13 planning cycle, these investment priorities are as follows:

- ISE-SAR Activities;
- State and Major Urban Area Fusion Centers;
- ITACG;
- SBU/CUI Framework Transition; and
- ISE Shared Spaces.

To better understand these investment priorities, the PM-ISE conducted a series of program reviews, requesting that ISE agencies provide cost data for FY 2007-09 associated with these priorities. The reviews were closely coordinated with OMB to ensure that the results could be incorporated into broader budget guidance. Based on the results, OMB issued direction to agencies on specific ISE priorities. Moving forward, the ISE will measure performance of each of these priorities as a portion of its performance management approach. These program reviews will continue next year to better align ISE investment and Performance management activities and facilitate the integration of ISE Investments and Performance Management initiatives into agency management structures through out-year planning and increased involvement of Performance Improvement Officers.

[37] IRTPA, as amended, op. cit., §1016 (h)(2)(C).

8 Promoting a Culture of Information Sharing

"Heads of executive departments and agencies must actively work to create a culture of information sharing within their respective departments or agencies by assigning personnel and dedicating resources to terrorism information sharing, by reducing disincentives to such sharing, and by holding their senior managers and officials accountable for improved and increased sharing of such information."

— Guidelines and Requirements in Support of the ISE, Requirement 2

Fostering an information sharing culture may be the most formidable challenge confronting the ISE. In the post-9/11 world, a predisposition to share the right information with those who need it is not merely an option but a fundamental principle firmly grounded in law and regulation. The goal is clear, but achieving it will take dedicated effort. The NSIS states "We will…change government culture to one in which information is regularly and responsibly shared and only withheld by exception." ISE cultural change initiatives aim to ensure that this principle is clearly understood and that managers are held accountable for driving change in their agencies.

8.1 2007-08 Progress

Accomplishments in 2007-08 include:

- Development of an ISE-wide computer based core awareness training course to be released to ISE participants this summer. The course will be distributed in one of three ways depending on agency preference:
  - As a program compatible with agencies' Learning Management systems;
  - As a program that can be installed directly on agencies' websites; or
  - On a compact disk that be installed at a user workstation.
- Following distribution of the course, Federal agencies will ensure that personnel who support the CT mission receive this core awareness training, tailoring it to their particular needs or supplementing it with agency-developed mission-specific training. Performance goals and measures to track progress will be incorporated in the 2008-09 Report.

In addition to the ISE Core Awareness Training, ISE participants are required to develop tailored training programs that achieve specific, related, learning objectives. One-third of the agencies surveyed in the fall indicated that they had established and completed some form of training to increase information sharing awareness. This number increased to 47% in the spring assessment.

- Many agencies—including DoD, DHS, and DNI—have issued new or first-time information sharing policies and strategies. The DNI's information sharing strategy, for example, is based on the premise of changing the IC from a "need to know" culture to one that embraces the principle of "responsibility to provide."
- DoD is assessing individual performance against information sharing practices and incorporating incentives into personnel processes and systems.
- Several organizations, including the ODNI and the Intelligence Division of the Department of Transportation, have incorporated information sharing as a factor in performance evaluations. Organizations are also beginning to include information sharing awards as part of departmental incentive programs. Overall participation improved from 40% last fall to 73% in this spring's performance assessment. As the DNI Information Sharing Strategy points out, "If … personnel perceive that professional success is based in part on how well they share information, sharing *will improve* [emphasis added]."

Last fall, 27% of ISE agencies ISC member agencies reported initial steps to ensure accountability for information sharing via performance appraisals. The number grew to 47% this spring, with several agencies requesting assistance from OPM.

- DHS provides recognition, cash awards, time off, and other rewards when information sharing leads to the identification or apprehension of an individual posing a threat to national security.
- Many ISC members have established information sharing management boards and promulgated polices to promote sharing through techniques such as "write to release" and have modified practices that inhibit information sharing.

In the fall assessment, 53% of agencies were able to identify steps they took to remove information sharing disincentives in the areas of document dissemination (e.g., reduced use of originator controls), writing for release, and policies for sharing between internal departments. This number increased to 73% for the spring assessment.

8.2 Next Steps

Programs intended to create cultures of sharing will continue to evolve in the upcoming months to influence employee performance appraisals, awards and incentives programs, training, and initial implementation of the *ISE Privacy and Civil Liberties Implementation Manual*. Planned activities include the following:

- Enabling personnel who support the CT mission to receive the core ISE awareness training as the core training modules are developed. This training will be tailored to particular needs of personnel or be supplemented with agency-developed, mission-specific training;

- Expanding information sharing training to include courses responding directly to ISE priorities such as SAR. In addition, training guidelines for SLT entities will be developed by DOJ and DHS in coordination with other ISC members; and
- Partnering with OPM to assist agencies in adding information sharing elements to performance appraisals and incorporating information sharing incentives into personnel practice.

9 2009 ISE Performance Goals

IRTPA requires "objective system-wide performance goals for the following year."[38] In compliance with this requirement, the 2009 Performance Goals focus on:

1. Ensuring further development of initiatives related to the Presidential Guidelines and Requirements that are not yet sufficiently mature (e.g., Foreign Government Information Sharing; implementation of ISE Privacy Guidelines);

2. Further evolution and agency implementation of initiatives related to the Presidential Guidelines and Requirements that are based on actual operations with cross-cutting priority mission areas including SAR and AWN; and

3. Agency focused implementation activities.

The goals are designed to determine (1) the activities required to achieve anticipated 2008-2009 ISE outcomes and (2) the objectives and measures to track progress against these planned implementation efforts (Table 9-1).

Upcoming ISE performance management efforts linking 2009 Performance Goals to supporting objectives and measures will bring the ISE even closer to complying with the Presidential guidelines and requirements and the NSIS. This linkage will also provide the PM-ISE and the ISC with a means to better determine whether ISE initiatives are having their intended effect. ISC member agencies will use this assessment to identify areas where they can better build their capacity for information sharing. A line of sight from the 2009 Performance Goals to further maturation of specific ISE activities identified in the President's Guidelines and Requirements will provide the PM-ISE and the ISC with data to demonstrate the ISE's value to the next Administration, Congress, and beyond.

Table 9-1. 2009 ISE Performance Goals

2009 ISE Performance Goals
To further create a culture of sharing, agencies will: • Ensure all personnel charged with sharing terrorism information complete ISE awareness training. • Make information sharing a factor in awards and incentives programs. • Add information sharing elements to employee performance appraisals. • Complete Stage 1 of the *ISE Privacy and Civil Liberties Implementation Manual*.
To further reduce barriers to sharing, agencies will: • Implement ISE Shared Spaces. • Begin to adopt the Controlled Unclassified Information (CUI) Framework. • Work toward security reciprocity among Federal/State/local and private sector entities, to include people facilities and systems.

[38] IRTPA, as amended, §1016(h)(2)(B).

2009 ISE Performance Goals
To improve sharing practices with Federal, State, local, tribal and foreign partners, agencies will: • Make the ITACG fully-functional. • Increase fusion centers' access to terrorism-related information and ISE capabilities. • Make available to the appropriate personnel tools and mechanisms for the negotiation of terrorism-related agreements and arrangements. • Complete initial efforts to establish a national process for suspicious activity reporting.
To institutionalize sharing, agencies will: • Further integrate their IT management structures with ISE Enterprise Architecture principles. • Adopt ISE standards. • Further integrate ISE investment and performance management initiatives into department and agency management structures through out-year planning and increased involvement of Performance Improvement Officers.

Appendix A – Summary of the Alignment Between the NSIS and ISE Accomplishments

National Strategy for Information Sharing Core Principles and Understandings[39]	Alignment to ISE Accomplishments
Effective information sharing comes through **strong partnerships among Federal, State, local, and tribal authorities, private sector organizations, and our foreign partners and allies**.	• Established the ITACG and initiated development of an integrated network of fusion centers to enable the effective sharing of terrorism-related information between Federal and SLT partners. • Provided common tools and mechanisms that assist departments and agencies in facilitating the sharing of terrorism information with foreign governments.
Information acquired for one purpose, or under one set of authorities, might provide unique insights when combined, in accordance with applicable law, with seemingly unrelated information from other sources, and therefore we must **foster a culture of awareness in which people at all levels of government remain cognizant of the functions and needs of others and use knowledge and information from all sources to support counterterrorism efforts**.	• Completed an ISE-wide information sharing training course to be available to ISC member agencies this summer. • Replaced of the restrictive Cold War tenet of "need to know" by the principle of "responsibility to provide." • Efforts underway or in place to include information sharing as an important factor in personnel evaluation and awards and incentives programs. • Worked with fusion centers and local law enforcement departments to integrate a standard ISE-Suspicious Activity Reporting (SAR) business process into the day-to-day operational environments of their region.
Information sharing **must be woven into all aspects of counterterrorism activity**, including preventive and protective actions, actionable responses, criminal and counterterrorism investigative activities, event preparedness, and response to and recovery from catastrophic events.	• Established the ISE standards program and published the first ISE functional standard that institutionalizes an integrated ISE SAR process. • Leveraged the fundamental concepts of the *ISE Enterprise Architecture Framework* (EAF) and *ISE Profile and Architecture Implementation Strategy* (PAIS) by DOJ, DHS, and others for applications broader than the ISE. • Established the CTISS program and issued the *ISE SAR Functional Standard*. CTISS are business process-driven, performance-based "common standards" for preparing terrorism information for maximum distribution and access within the ISE. The SAR Functional Standard provides the data and information sharing foundation for operational information sharing of SAR in the ISE and supports demonstrations to include the SAR Evaluation Environments and an effort by the LAPD to redefine its SAR law enforcement processes. • Demonstrated the ISE EAF and CTISS in operational pilots. • Incorporated the ISE performance and investment strategy to provide the programmatic foundation for further institutionalizing the ISE.

[39] NSIS, op. cit., p. 2.

National Strategy for Information Sharing Core Principles and Understandings[39]	Alignment to ISE Accomplishments
The procedures, processes, and systems that support information sharing must **draw upon and integrate existing technical capabilities and must respect established authorities and responsibilities**.	• Released the ISE EAF, a strategic guide for mapping ISE participants' enterprise architectures into the Government's FEA. The ISE-EAF provides a roadmap to enable long-term, institutionalized technology improvement and information systems planning, investing, and integration to support the sharing of terrorism-related information and identifies the network interfaces and standards needed to facilitate information sharing. • Ensuring that the CTISS Program incorporates information exchange standards developed for CTISS by DOJ's and DHS's NIEM program office into new ISE-wide functional standards.
State and major urban area fusion centers represent a valuable information sharing resource and **should be incorporated into the national information sharing framework**, which will require that fusion centers achieve a baseline level of capability to gather, process, share, and utilize information and operate in a manner that respects individuals' privacy rights and other legal rights protected by U.S. laws.	• Supporting improved collaboration at the State and local levels by leveraging fusion centers "as the primary focal points within the State and local environment for the receipt and sharing of terrorism-related information" and by establishing and sustaining a national integrated network of these centers

Appendix B – Acronyms and Abbreviations

AWN	Alerts, Warnings, and Notifications
ARJIS	Automated Regional Justice Information System
BJA	Bureau of Justice Assistance
C&A	Certification and Accreditation
CA	California
CI/KR	Critical Infrastructure/Key Resources
CICC	Criminal Intelligence Coordinating Council
CIIMS	Critical Infrastructure Inspection Management System
CIO	Chief Information Officer
CJIS	Criminal Justice Information Services
CP	Counterproliferation
CT	Counterterrorism
CTISS	Common Terrorism Information Sharing Standards
CUI	Controlled Unclassified Information
DHS	Department of Homeland Security
DNI	Director of National Intelligence
DoD	Department of Defense
DOJ	Department of Justice
EA	Enterprise Architecture
EAF	Enterprise Architecture Framework
EU	European Union
FBI	Federal Bureau of Investigation
FEA	Federal Enterprise Architecture
FIPS	Federal Information Processing Standard
FY	Fiscal Year
HIR	Homeland Intelligence Reports
HSDN	Homeland Security Data Network
HSIN	Homeland Security Information Network
IA	Information Assurance
IACP	International Association of Chiefs of Police
IC	Intelligence Community
ICE	Immigration and Customs Enforcement
ICEPIC	ICE Pattern Analysis and Information Collection System
IEPD	Information Exchange Package Description
IP	Implementation Plan
IRTPA	Intelligence Reform and Terrorism Prevention Act of 2004

ISC	Information Sharing Council
ISE	Information Sharing Environment
ISE EAF	Information Sharing Environment Enterprise Architecture Framework
IT	Information Technology
ITACG	Interagency Threat Assessment and Coordination Group
JTTF	Joint Terrorism Task Force
LAPD	Los Angeles Police Department
LE	Law Enforcement
LEO	Law Enforcement Online
LES	Law Enforcement Sensitive
LEISP	Law Enforcement Information Sharing Program
LEXS	LEISP Exchange Specification
LInX	Law Enforcement Information Exchange
MSP	Maryland State Police
NARA	National Archives and Records Administration
NCIS	Naval Criminal Investigative Service
NCTC	National Counterterrorism Center
N-DEx	National Data Exchange
NFCCG	National Fusion Center Coordination Group
NIEM	National Information Exchange Model
NIPP	National Infrastructure Protection Plan
NIST	National Institute of Standards and Technology
NSIS	National Strategy for Information Sharing
NSS	National Security Systems
ODNI	Office of the Director of National Intelligence
OMB	Office of Management and Budget
OPM	Office of Personnel Management
PAIS	Profile and Architecture Implementation Strategy
PDA	Personal Digital Assistant
PGC	Privacy Guidelines Committee
PM-ISE	Program Manager, Information Sharing Environment
R-DEx	Regional Data Exchange
RISS	Regional Information Sharing System
SAR	Suspicious Activity Reporting
SBU	Sensitive But Unclassified
SCI	Sensitive Compartmented Information
SIPRNET	Secret Internet Protocol Router Network
SLIAG	Senior Level Interagency Advisory Group
SLT	State, Local, and Tribal

TIDE	Terrorist Identities Datamart Environment
TN-ISPP	Tribal Nations Information Sharing Pilot Project
TSC	Terrorist Screening Center
TSDB	Terrorist Screening Database
TWPDES	Terrorist Watchlist Person Data Exchange Standard
TX	Texas
UCORE	Universal Core
U.S.	United States
WA	Washington
WMD	Weapons of Mass Destruction
WMD-T	Weapons of Mass Destruction – Terrorism-Related

Office of the Director of National Intelligence
Attention: Program Manager, Information Sharing Environment
Washington, D.C. 20511

(202) 331-2490

Visit us on the web at http://www.ise.gov